Guardians at the Gates of Hell

Estimating the Risk of Nuclear Theft and Terrorism –
and Identifying the Highest-Priority Risks of Nuclear Theft

by

Matthew Bunn
SB and SM, Political Science, MIT, 1985

SUBMITTED TO THE ENGINEERING SYSTEMS DIVISION IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN TECHNOLOGY, MANAGEMENT, AND POLICY AT THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JANUARY 2007
[June 2007]

SIGNATURE OF AUTHOR.....
Technology, Management and Policy Program, Engineering Systems Division

CERTIFIED BY.....
Richard K. Lester
Professor of Nuclear Engineering, Committee Chairman

CERTIFIED BY.....
Graham T. Allison
Douglas Dillon Professor of Government
John F. Kennedy School of Government, Harvard University

CERTIFIED BY.....
John P. Holdren
Teresa and John Heinz Professor of Environmental Policy
John F. Kennedy School of Government, Harvard University

CERTIFIED BY.....
Marvin Miller
Senior Scientist Emeritus, Nuclear Engineering

ACCEPTED BY.....
Richard de Neufville
Professor of Engineering Systems
Chairman, Educational Policy Committee, Engineering Systems Division

Guardians at the Gates of Hell:
Estimating the Risk of Nuclear Theft and Terrorism –
and Identifying the Highest-Priority Risks of Nuclear Theft

by

Matthew Bunn

Submitted To The Engineering Systems Division on January 31, 2007 in Partial Fulfillment of the Requirements for the Degree of Doctor Of Philosophy in Technology, Management, and Policy

ABSTRACT

Methods are presented to assess the global risk of nuclear theft and nuclear terrorism, to identify the nuclear facilities and transport legs that pose the highest-priority risks of nuclear theft, and to evaluate policy approaches to strengthening security and accounting for nuclear stockpiles worldwide. First, a qualitative assessment outlines the demand for black-market nuclear weapons and materials; the plausibility of terrorist construction of an improvised nuclear device; the global stocks and flows of nuclear weapons, plutonium, and highly enriched uranium (HEU), with the global distribution of facilities where they exist; and the widely varying standards of physical protection, control, and accounting in place to prevent theft. Particular dangers of nuclear theft in Russia, Pakistan, and from HEU-fueled research reactors are highlighted. Second, a mathematical model of the global risk of nuclear terrorism is presented, with detailed assessments of what is known about the values of each of the parameters, and of policies that could change each of the parameters to reduce risk. Third, a methodology for identifying the nuclear facilities and transport legs posing the highest risks of nuclear terrorism is presented, combining the security levels for each facility or transport leg, the levels of threat they face, and the quantity and quality of nuclear weapons or weapons-usable material they contain. Fourth, the global nuclear security system is described and assessed as a complex, large-scale, integrated, open system (CLIOS). Based on past experiences with different policy tools from negotiated international standards to on-the-ground technical cooperation to install improved security equipment, options to improve system performance in reducing the risk of nuclear terrorism are assessed. A final chapter offers conclusions and recommendations.

Commmittee chair: Richard K. Lester, Professor of Nuclear Engineering

Committee member: Graham T. Allison, Douglas Dillon Professor of Government John F. Kennedy School of Government, Harvard University

Committee member: John P. Holdren, Teresa and John Heinz Professor of Environmental Policy, John F. Kennedy School of Government, Harvard University

Committee member: Marvin Miller, Senior Scientist Emeritus, Nuclear Engineering

ACKNOWLEDGEMENTS

The research for this dissertation was supported by a book grant from the Japan Foundation Center for Global Partnership. The study is based on years of research which have been made possible through the generous support of the Nuclear Threat Initiative, the Ploughshares Fund, and the John D. and Catherine T. MacArthur Foundation. I would especially like to thank my father, George Bunn, for his generous, insightful, and patient support for this effort.

I would like to thank the members of my committee, Richard K. Lester (chairman), Graham T. Allison, John P. Holdren, and Marvin Miller, for their comments, suggestions, and support. I would also like to thank the many other colleagues and mentors who have helped shape my thinking on these subjects over the years, especially Frank von Hippel, Ashton B. Carter, Rose Gottemoeller, Kenneth N. Luongo, William Potter, and my colleagues at the Belfer Center and the Nuclear Threat Initiative. Thanks are due also to the many officials of the U.S. and Russian governments and international organizations, as well as experts at U.S. and Russian nuclear facilities, who gave generously of their time in discussions of these critical issues. These officials and experts prefer to remain anonymous. Richard de Neufville and John Lathrop of Lawrence Livermore National Laboratory provided valuable comments on an earlier draft of Chapter 3.

Anthony Wier, my research partner and co-author for the past several years, deserves special thanks. He has shaped my thinking in innumerable ways; he contributed to earlier papers that several portions of this dissertation draw from; and he provided invaluable advice on both substantive matters and the finer points of word processing and spreadsheet calculations. Thanks are due also to Patricia McLaughlin of the Science, Technology, and Public Policy Program at Harvard's Kennedy School of Government, who provided daily support with unflagging good humor.

Most importantly, I would like to thank my wonderful wife Jennifer Weeks, and our daughters Claire and Nina, for being the joy and inspiration of my life, and for their love and patience as this project dragged on. This dissertation is dedicated to them, in the hope that Claire and Nina may enjoy a safer world.

All responsibility for any errors and misjudgments is solely my own.

AUTHOR BIOGRAPHY

Matthew Bunn is a Senior Research Associate in the Project on Managing the Atom in the Belfer Center for Science and International Affairs at Harvard University's John F. Kennedy School of Government. His current research interests include nuclear theft and terrorism; nuclear proliferation and measures to control it; and the future of nuclear energy and its fuel cycle.

Before joining the Kennedy School in January 1997, he served for three years as an adviser to the Office of Science and Technology Policy, where he played a major role in U.S. policies related to the control and disposition of weapons-usable nuclear materials in the United States and the former Soviet Union and directed a secret study for President Clinton on security for nuclear materials in Russia. Previously, Bunn was at the National Academy of Sciences, where he directed the two-volume study Management and Disposition of Excess Weapons Plutonium.

He is the winner of the American Physical Society's Joseph A. Burton Forum Award for "outstanding contributions in helping to formulate policies to decrease the risks of theft of nuclear weapons and nuclear materials," and is an elected Fellow of the American Association for the Advancement of Science. He is a member of the Boards of Directors of the Arms Control Association and the Partnership for Global Security, and serves on the Committee on the Internationalization of the Nuclear Fuel Cycle, a joint committee of the U.S. National Academy of Sciences and the Russian Academy of Sciences. Previously, he served on the Nonproliferation Advisory Panel to the Director of Central Intelligence. He is a consultant to the Nuclear Threat Initiative, and previously consulted for the Lawrence Livermore National Laboratory, Bechtel National, and others.

Bunn is the author or co-author of a dozen books and book-length technical reports (most recently including *Securing the Bomb 2006*), and scores of articles in publications ranging from *Science* and *Nuclear Technology* to *Foreign Policy* and *The Washington Post.* He appears regularly on television and radio.

Bunn received his bachelors' and masters' degrees in political science, specializing in defense and arms control, from the Massachusetts Institute of Technology in 1985. He is married to Jennifer Weeks. They have two daughters, Claire and Nina.

Table of Contents

List of Figures

List of Tables

1. Introduction

The inspectors arrived at the sprawling nuclear weapons assembly and disassembly facility on a Thursday in October, to review the facility's security measures. They were surprised by what they found. There was no portal monitor at the gate to detect nuclear material being smuggled out, and no metal detector to prevent guns from being smuggled in. In a test, inspectors playing the roles of thieves (including an insider) succeeded in smuggling out enough mock nuclear material for a bomb. The facility was immediately closed for security upgrades. It reopened the following Tuesday, with nuclear material detectors and metal detectors in place.

This was not Russia in 1995. It was the United States in 1985. The facility was Pantex, the United States' main plant for putting together and taking apart nuclear weapons, in Amarillo, Texas – intended to be perhaps the highest-security nuclear site in the United States, if not the world.[1] The Pantex inspection took place just after a special project team had finished urgently reviewing security at every site in the U.S. nuclear weapons complex managed by the Department of Energy (DOE). The team found scores of serious security vulnerabilities and made 94 recommendations for action to improve security throughout the DOE complex. The Secretary of Energy at the time launched a major initiative to implement the steps the team called for – an effort that was dubbed Operation Cerberus, after the mythological guardian of the gates of hell. Most of the team's recommendations were implemented within less than a year, and nearly all were carried out within a few years, at an estimated cost of $1.5 billion. The result was substantially and demonstrably improved security – miles of impressive razor-wire fences installed, major barriers put in place, upgraded access controls installed, guard forces beefed up, and more.[2] Yet within a few years, complacency was creeping back, security budgets were being cut, and DOE security managers were warning that if immediate actions were not taken to correct the decline, nuclear weapons and materials could not be adequately secured.[3]

---

[1] For discussions of the Pantex test (and others revealing remarkable vulnerabilities) see Committee on Energy and Commerce, *Nuclear Weapons Facilities: Adequacy of Safeguards and Security at Department of Energy Nuclear Weapons Production Facilities*, U.S. Congress, House of Representatives, 99th Congress, 2nd Session, 6 March 1986. See, in particular, pp. 182-187.

[2] For discussions of the special project team and Operation Cerberus, see *Nuclear Weapons Facilities*, pp. 39-54; National Research Council, *Material Control and Accounting in the Department of Energy's Nuclear Fuel Complex* (Washington, DC: National Academy Press, 1989), pp. 30-31; John B. Roberts, II, "Nuclear Secrets and the Culture Wars," *American Spectator* 32, no. 5 (May 1999), pp. 34-39, 76. The $1.5 billion figure is from the *American Spectator* account, which is an attack on allegedly lax security measures in the Clinton years, and holds up Operation Cerberus as a counter-example from the Reagan years. The notion that all was well with DOE security in the Reagan and Bush years does not stand up to the scrutiny provided in *Nuclear Weapons Facilities*; President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington D.C.: PFIAB, 1999; available at http://www.fas.org/sgp/library/pfiab/ as of 13 December 2006).

[3] By 1991, for example, DOE's annual report to the President on safeguards and security in the DOE complex was warning that "significant improvements must be made immediately"; by 1996, the annual report was warning of "severe budget reductions... which have undermined protection of special nuclear material." Both

Fast forward two decades, to a world in which extreme Islamist terrorists are actively seeking nuclear weapons and their essential ingredients – yet weapons-usable nuclear materials and even nuclear weapons themselves in countries around the world are, in some cases, dangerously insecure. Operation Cerberus was aptly named, for, as this dissertation will argue, security measures to prevent nuclear weapons and materials from being stolen are the most important gate barring the path to the hell of nuclear terrorism.

The urgent questions about nuclear terrorism that this dissertation attempts to answer are "how big is the risk?" and "what policy measures would be most effective in reducing it?" Unfortunately, the answers to both are "no one knows for sure." To help clarify the debate over these questions, this dissertation will provide both qualitative and quantitative methods for assessing the risk of nuclear terrorism; a methodology for identifying those nuclear facilities and transport legs worldwide that pose the most urgent risks that nuclear weapons or their essential ingredients could be stolen and fall into terrorist hands; and a description of the complex global system of nuclear security (with its ingrained resistance to major policy changes), with suggestions, based on past experience, of how best to achieve higher levels of security for nuclear stockpiles around the world.

In essence, in this dissertation I seek to provide at least the beginnings of answers to three questions:

- How big is the risk of nuclear terrorism?
- How can we identify the nuclear facilities and transport legs whose vulnerabilities contribute most to that risk?
- What policy initiatives are likely to be most effective in improving the performance of the complex global nuclear security system in reducing this risk?

Estimating the Risk of Nuclear Terrorism

The importance of these questions can hardly be overstated. The one topic President George W. Bush and Senator John Kerry agreed on in their Presidential contest in 2004 was that the danger that terrorists could get and use a nuclear bomb was the biggest current threat to the security of the United States.[4] President Bush has said that this danger is urgent enough to justify doing "everything in our power" to prevent it.[5] The 9/11 Commission made the same point, calling for a "maximum effort" to prevent proliferation of weapons of mass destruction, and particularly nuclear weapons, to terrorists.[6] Mohammed ElBaradei, the

---

reports are quoted in the depressing appendix listing reviews of DOE security in President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst.*

[4] "The First Bush-Kerry Presidential Debate, University of Miami, Coral Gables, Florida," *Commission on Presidential Debates*, 30 September 2004.

[5] President George W. Bush, "President Delivers 'State of the Union'" (Washington, D.C.: The White House, Office of the Press Secretary, 28 January 2003; available at http://www.whitehouse.gov/news/releases/2003/01/20030128-19.html as of 30 December 2006).

[6] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 1st ed. (New York: Norton, 2004; available at http://www.gpoaccess.gov/911/index.html as of 30 December 2006), p. 381.

Director-General of the International Atomic Energy Agency (IAEA) recently went so far as to warn that the world is in "a race against time" to prevent nuclear terrorism – in essence, a race to lock down nuclear stockpiles around the world before terrorists and thieves can get to them.[7]

Not everyone agrees, however. In many capitals, political leaders believe the United States has been engaged in needless fear-mongering in focusing on terrorists gaining the ability to set off crude nuclear bombs as a realistic threat. Karl-Heinz Kamp, a prominent European analyst, expressed the view held by many: "religious zealots or political extremists may present many dangers, but wielding nuclear bombs and killing hundreds of thousands of innocent people is not one of them."[8] This view is widespread in the nuclear industry itself. As the deputy director for security of Rosatom, Russia's nuclear agency, put it, "we have to bear it in mind that even having any nuclear material does not mean that an explosive device can be made [by terrorists]. This is absolutely impossible."[9] Quantitatively, well-informed observers have made estimates of the probability of terrorist use of a nuclear bomb on a major city in the next decade that range from 1% to 50% or more (though as we will see in Chapter 3, even a 1% probability would be sufficient to justify major efforts to reduce the risk).[10]

This dissertation uses both qualitative and quantitative approaches to elucidate the issues in this debate over the size of the nuclear terrorism risk. First, it provides a qualitative assessment, detailing several points:

- It is plausible that a capable terrorist group would be able to make at least a crude nuclear bomb if they acquired the needed highly enriched uranium (HEU) or plutonium;
- Such weapons-usable nuclear materials are inadequately secured at scores of sites around the world (as are nuclear weapons themselves, in some cases);
- The al Qaeda terrorist network and elements of the global movement it has spawned have made repeated attempts to get nuclear bombs or weapons-usable nuclear materials to make them, and they have repeatedly tried to recruit nuclear weapon scientists to help them; and

---

[7] "Race against Time to Prevent Nuclear Terror - IAEA," *Reuters*, 8 November 2004.

[8] Karl-Heinz Kamp, "Nuclear Terrorism Is Not the Core Problem," *Survival* 40, no. 4 (Winter 1998).

[9] Aleksandr Khinshteyn, "Secret Materials," trans. BBC Monitoring Service, "Russian Central TV," 29 November 2002.

[10] Both Graham Allison and former Secretary of Defense William Perry have put the probability of a terrorist nuclear attack within the next decade at about 50 percent. See Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004); Nicholas D. Kristof, "An American Hiroshima," *New York Times*, 11 August 2004. By contrast, David Albright, who has written some of the most detailed unclassified analyses of seized al Qaeda nuclear documents, puts the ten-year probability in the range of 1%. See Corine Hegland and Gregg Webb, "The Threat," *National Journal* 37, no. 16 (15 April 2005; available at http://nationaljournal.com/about/njweekly/stories/2005/0415nj1.htm as of 30 December 2006). For a poll of leading national security and foreign policy experts on this and related points, see Richard G. Lugar, *The Lugar Survey on Proliferation Threats and Responses* (Washington, D.C.: Office of Senator Lugar, 2005; available at http://lugar.senate.gov/reports/NPSurvey.pdf as of 2 January 2007).

- Nuclear materials are so difficult to detect – and the borders of modern states so porous – that only modest reliance can be placed on measures to prevent nuclear weapons and materials from being smuggled into a country.

At the same time, however, this chapter makes the point that, more than a decade after the collapse of the Soviet Union and after the launch of al Qaeda's attempts to get nuclear weapons, there is no compelling evidence that either a nuclear bomb or the materials to make one have fallen into the hands of terrorist groups. Moreover, none of the fragmentary evidence publicly available suggests that either the Japanese cult Aum Shinrikyo nor al Qaeda – the two terrorist groups which have focused the most effort on acquiring nuclear ewapons – have come close to putting together the capabilities needed to make a nuclear bomb.

That qualitative assessment indicates that the point at which policy measures have their greatest leverage in reducing this threat is in keeping nuclear weapons and materials from being removed from the sites where they are supposed to be in the first place – for once they have been stolen, they could be anywhere, and the problem of finding them and preventing their use increases by orders of magnitude. Hence, ensuring that all of the world's stockpiles of nuclear weapons and materials are effectively secured against the threats that terrorists and thieves have shown they can pose is central to the security of every country and to the global effort to stem the spread of nuclear weapons. A range of programs are underway to help countries improve security for their nuclear stockpiles, and these efforts have had real and demonstrable successes. But as of late 2006, only a fraction of the nuclear stockpiles around the world that are believed to be vulnerable have received substantial security upgrades. As previous work has made clear, the scale and pace of these efforts fall far short of meeting President Bush's "everything in our power" strandard.[11]

Second, this dissertation takes a quantitative approach to the same problems, presenting and analyzing a mathematical model of the global risk of nuclear terrorism.[12] After presenting the mathematical model, I offer a numerical example of the use of the model; explore what is known from the historical record or from other sources about the likely value of each of the parameters in the model; outline policies that might change the values of these parameters so as to reduce risk; and identify information whose collection and analysis could reduce the current uncertainty in estimating the values of those parameters. This quantitative approach provides a basis for highlighting the specific sources of disagreement about the overall magnitude of the risk, a tool for assessing the potential impact of alternative policies, and a structure for a research agenda to further clarify the risk and the effectiveness of possible responses.

---

[11] For an assessment of progress in securing nuclear stockpiles as of the spring of 2006, see Matthew Bunn and Anthony Wier, *Securing the Bomb 2006* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2006; available at http://www.nti.org/securingthebomb as of 23 July 2006). The current pace and scope of these efforts is not assessed in detail in this dissertation.

[12] Throughout this dissertation, I define risk as the probability of an event times its consequences, rather than attempting any more subtle or complex approach.

Identifying the Highest-Priority Risks of Nuclear Theft

In a world of limited resources – not only of money and people, but also of political attention to particular issues – how can the facilities that pose the highest-priority security risks of nuclear theft, requiring the most immediate attention, be identified? When officials at the IAEA, in the U.S. government, or in other donor states are seeking to allocate resources for reducing the risk of nuclear theft and terrorism, what criteria should be used to determine whether a small civilian facility in Western Europe, with enough HEU for one or a few bombs and few guards, or a nuclear weapons facility in Pakistan, which is heavily guarded but in an area where substantial armed remnants of al Qaeda continue to operate, poses a more urgent risk to be addressed?

To some extent, the answers to such questions will always remain matters of judgment – particularly judgment on matters such as whether a large armed attack by outsiders or a covert theft attempt by insiders poses a more likely and worrisome threat at particular facilities. But the grounds for uncertainty and debate in setting priorities can be greatly reduced – and high-risk facilities that might otherwise go unnoticed can be identified – by applying a rigorous framework for assessing risk. This dissertation lays out such a framework, based on the *quantity* of nuclear material at a site, the *quality* of that material (in particular, how difficult it would be for different types of groups to make it into a bomb), the effectiveness of the *security and accounting arrangements* at the site, and the level of *threat* in the area of that site (such as the presence of organized terrorist activity, the incidence of theft and corruption, pay and morale among the facility's employees, and the like). Between them, these factors make it possible to assess how the probability that nuclear material would be stolen from a particular site and the probability that it could then be turned into a nuclear bomb compares to those probabilities at other sites. (This approach only allows a ranking of risk among different sites, not a calculation of the absolute magnitude of the probability of nuclear theft and terrorism, because of the very large uncertainties in judging the probability that theft will even be attempted at any particular site and the substantial uncertainties in the other elements of the assessment.)

Using the limited data that are publicly available, I then assess nuclear theft risks in several countries, as an example of the application of the method. This assessment makes clear that some of today's most urgent theft risks are in Russia (where the world's largest and most widely dispersed nuclear stockpiles have security measures that have improved from poor to medium over the past decade and face high levels of threat, from both outside terrorist attackers and insider thieves) and in Pakistan (whose nuclear stockpile is relatively small and heavily guarded, but is exposed to enormous threats both from armed terrorist groups in the country and from nuclear insiders with a demonstrated willingness to sell sensitive weapons-related technologies). Research reactors fueled with highly enriched uranium (many of which have enough HEU for a nuclear bomb, with very little security) also pose significant risks. Of course, as one government or facility operator may be far more cooperative than another, in setting priorities for action it is important to consider not only where the most urgent risks lie, but also where the greatest opportunities for action may be – and this balance is addressed as well.

For this question, the dissertation applies a technology assessment methodology, assessing how difficult it would be for threats of different types to overcome varying security and accounting arrangements to steal nuclear weapons or nuclear materials and then assessing how the quantity and characteristics of the material that might be stolen affects the probability that different types of groups or states could use that nuclear material to make a usable nuclear explosive.

Understanding the Global Nuclear Security System and Options for Change

To achieve the goal of improving nuclear security arrangements quickly and effectively it will be necessary to use effective policy tools for meeting that objective, and these have to be identified. The United States and a number of other countries have now been cooperating with the states of the former Soviet Union to improve nuclear material security since 1993 – more than ten years. Other international efforts to improve security for nuclear stockpiles stretch back decades. Hence, there is now a substantial base of experience to learn from, in determining which approaches appear to work best – and under what particular circumstances.

To provide a framework for analyzing the lessons of these past experiences and understanding the likely effectiveness of different future initiatives, it is important to understand the global nuclear security system as it has evolved and responded to past pressures. Global nuclear security is a classic complex, large-scale, integrated, open system (CLIOS).[13] It is *complex* in the sense that the system involves hundreds of different components, whose interactions are not fully understood; it is *large-scale* in that it involves hundreds of facilities in over forty countries managing tens of thousands of nuclear weapons and thousands of tons of weapons-usable nuclear material; it is *integrated* in the sense that each component is significantly influenced by the behavior of other components, with links of influence (albeit weak ones, in many cases) stretching across the globe; and it is *open* in the sense that the physical systems of fences and barriers and guards interact in crucial ways with policy systems of regulation, financial decisions, and the like, and the total system is deeply influenced by, and poses risks to, the rest of society in countries around the world.

In this dissertation I present an assessment of the shape and behavior of this system and in particular the factors that cause and constrain changes in the system's overall performance in providing high levels of nuclear security. I then review the record of various policy tools for improving the nuclear security system's performance, rating their effectiveness using a consistent set of criteria and drawing lessons for future initiatives from the record of each policy tool.

---

[13] For an introduction of the CLIOS concept, see Joseph M. Sussman, "Toward Engineering Systems as a Discipline" (Cambridge, MA: Massachusetts Institute of Technology, Engineering Systems Division, 6 September 2000; available at http://esd.mit.edu/wps/esd-wp-2000-01.pdf as of 30 December 2006).

Literature Review

The Risk of Nuclear Terrorism

There is an extensive literature on the threat of nuclear terrorism. It is often forgotten that this literature, and high-level concern about the danger of nuclear terrorism, stretches back more than thirty years, to a time long before the fears over "loose nukes" provoked by the collapse of the Soviet Union. John McPhee's 1974 book *The Curve of Binding Energy: A Journey into the Awesome and Alarming World of Theodore B. Taylor* presented a frightening description of how straightforward it would be for terrorists to make a nuclear bomb if they managed to get either plutonium or HEU, all described vividly by Taylor, one of the world's leading nuclear weapons designers.[14] Taylor's own book with Mason Willrich, *Nuclear Theft: Risks and Safeguards,* provides additional analysis and details, particularly with respect to approaches to reducing the threat.[15] The issue had arisen even earlier, however: a 1967 report by an Atomic Energy Commission advisory committee chaired by Ralph F. Lumb, *Report of the Advisory Panel on Safeguarding Special Nuclear Materials,* was the first published U.S. government document that specifically called out the need to protect nuclear weapons and weapons-usable materials against theft by "terrorist or criminal groups."[16] In 1977, the U.S. Congress' Office of Technology Assessment, in its report *Nuclear Proliferation and Safeguards*, provided one of the earliest and most perceptive official, unclassified summaries of what would be required for terrorists to make and use a crude nuclear bomb.[17] Years later, the 1987 book resulting from the work of the International Task Force on Prevention of Nuclear Terrorism provided probably the best available unclassified summary of the issue from the period before the collapse of the Soviet Union.[18]

During this early period, the literature included a great deal of concern over the then-expected "plutonium economy" and the risks of nuclear theft that might be associated with very large-scale use of separated plutonium. By the year 2000, it was expected that some 20,000 people in the United States alone would have access to separated plutonium in the civilian nuclear power industry.[19] The potential for theft or state diversion of plutonium has been a consistent theme of discussions of reprocessing and recycling ever since, and remain

---

[14] John McPhee, *The Curve of Binding Energy: A Journey into the Awesome and Alarming World of Theodore B. Taylor* (New York, NY: Farrar, Strauss, & Giroux, 1974). Some of the specific descriptions of how easy it would be to make various types of nuclear explosives in this book are overstated.

[15] Mason Willrich and Theodore B. Taylor, *Nuclear Theft: Risks and Safeguards* (Cambridge, MA: Ballinger, 1974). Another useful early account of the issue is Robert B. Leachman and Phillip Althoff, *Preventing Nuclear Theft: Guidelines for Industry and Government* (New York: Praeger, 1972).

[16] Ralph Lumb, *Report of the Advisory Panel on Safeguarding Special Nuclear Materials* (Washington, DC: Atomic Energy Commission, 1967).

[17] U.S. Congress, Office of Technology Assessment, *Nuclear Proliferation and Safeguards* (Washington, D.C.: OTA, 1977; available at http://www.wws.princeton.edu/ota/disk3/1977/7705/7705.PDF as of 12 December 2006).

[18] Paul Leventhal and Yonah Alexander, *Preventing Nuclear Terrorism* (Lexington, MA: Lexington, 1987).

[19] See, for example, U.S. Congress, *Nuclear Proliferation and Safeguards*, pp. 199, 243-245.

an important part of debates over the future of nuclear energy and its fuel cycle.[20] The likely effects on the risks of nuclear theft of increasing the number of sites where weapons-usable nuclear materials are handled, of increasing the number of people with access to such materials, and of increasing the total quantity of such materials in circulation are discussed in Chapter 3 of this dissertation. Beyond that, however, the dissertation does to delve deeply into the long-term future of nuclear energy and its impact on risks of nuclear proliferation and nuclear terrorism.

After the Soviet collapse, as stolen plutonium and HEU began appearing in Europe, the issue of potential nuclear terrorism came to the fore again. Aum Shinrikyo's 1995 sarin gas attack, as the first major, well-documented and well-publicized use of a particularly deadly weapon of mass destruction by a terrorist group, crossed a psychological barrier and highlighted the threat. Osama bin Laden has made his desire for nuclear weapons clear in public statements. Al Qaeda launched a focused effort to get such weapons and the materials and expertise to make them long before the 9/11 attacks, and this effort has continued since the destruction of al Qaeda's Afghan sanctuary. Aum Shinrikyo made numerous mistakes in its chemical and biological weapons efforts, which greatly reduced the casualties that the 1995 attack and other attempted Aum attacks might otherwise have caused. The 9/11 attacks, by contrast, crossed another threshold, in demonstrating that those whose ideas led them to want to kill huge numbers of civilians might sometimes be rational enough to carry out effective means for doing so.

In the years immediately following the Soviet collapse, the nuclear terrorism literature focused almost exclusively on the security for nuclear stockpiles in the former Soviet Union. The 1991 Harvard report *Soviet Nuclear Fission* offered an early summary of the dangers resulting from the then-imminent breakup of the Soviet Union and provided part of the basis for the establishment of the Nunn-Lugar program to address those dangers.[21] The follow-up study also highlighted the potential dangers of loss of nuclear control in the aftermath of the Soviet breakup and devoted a chapter to examining what should be done with excess nuclear material in particular.[22] A two-volume study from the U.S. National Academy of Sciences similarly focused on what should be done with nuclear material no longer needed for military purposes, but made clear that a broader regime to secure all plutonium and HEU worldwide to stringent standards was urgently needed.[23]

---

[20] For a recent discussion, see, for example, Matthew Bunn, testimony in Committee on Appropriations, Subcommittee on Energy and Water, *Global Nuclear Energy Partnership*, U.S. Senate, 109th Congress, 2nd Session, 14 September 2006.

[21] Kurt M. Campbell et al., *Soviet Nuclear Fission: Control of the Nuclear Arsenal in a Disintegrating Soviet Union* (Cambridge, MA: Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 1991).

[22] Graham Allison et al., *Cooperative Denuclearization: From Pledges to Deeds* (Cambridge, MA: Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 1993).

[23] U.S. National Academy of Sciences, Committee on International Security and Arms Control, *Management and Disposition of Excess Weapons Plutonium* (Washington, D.C.: National Academy Press, 1994; available at http://books.nap.edu/html/plutonium/0309050421.pdf as of 30 December 2006); U.S. National Academy of Sciences, Panel on Reactor-Related Options, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options* (Washington, D.C.: National Academy Press, 1995; available at http://books.nap.edu/

Within the U.S. government, two secret studies in early 1995 were particularly influential in highlighting the dangers posed by insecure nuclear materials and the inadequacies of then-current U.S. government efforts to address the problem. The first was a survey of nuclear security in the former Soviet Union prepared by the Joint Atomic Energy Intelligence Committee (JAEIC), which concluded that not a single facility in the former Soviet Union had adequate safeguards in place to protect against nuclear theft.[24] The second was a report from a high-level panel of the President's Committee of Advisers on Science and Technology (PCAST), which outlined the threat in stark terms and made a series of sweeping recommendations for action to address it, many of which were incorporated in a secret Presidential Decision Directive (PDD-41) in September 1995.[25] In 1996, Harvard's Belfer Center for Science and International Affairs published *Avoiding Nuclear Anarchy,* outlining the danger posed by insecure nuclear materials in stark terms, with a wealth of detail.[26] During this period, there were also a number of important journal and magazine articles, particularly from, for example, William C. Potter and his colleagues at Monterey's Center for Nonproliferation Studies; Frank von Hippel and his colleagues from Princeton University's Program on Nuclear Policy Alternatives; and Thomas B. Cochran and Christopher Paine from the Natural Resources Defense Council.[27]

As time went on, the literature began to reflect more focus on terrorists and what they might want to accomplish (and be able to accomplish) with weapons of mass destruction; as a result, the literature became less narrowly focused on the specific case of nuclear security and insecurity in the former Soviet Union (although that remained an important issue with a

---

html/plutonium/0309051452.pdf as of 30 December 2006). I directed this study; Wolfgang K.H. Panofsky chaired the plutonium study and John P. Holdren (one of the present committee members) chaired the committee and the panel.

[24] In unclassified 1996 testimony, then-Director of Central Intelligence John Deutch described this conclusion as the result of a "comprehensive evaluation" by the intelligence community, without mentioning the classified JAEIC study specifically. See Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction, Part II*, U.S. Senate, 104th Congress, 2nd Session, 13, 20, and 22 March 1996.

[25] Panel on U.S.-FSU Cooperation to Protect, Control, and Account for Weapons-Usable Nuclear Materials, President's Committee of Advisors on Science and Technology, *Securing Weapons-Usable Nuclear Materials in the Former Soviet Union: Urgent Measures to Prevent Nuclear Proliferation (U).* Secret/Noforn (Washington, D.C.: Office of Science and Technology Policy, 1995). I directed this study; John P. Holdren chaired it. For a summary of the report's recommendations, see Holdren's testimony in Committee on Foreign Relations, Subcommittee on European Affairs
Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Loose Nukes, Nuclear Smuggling, and the Fissile Material Problem in Russia and the NIS*, U.S. Senate, 104th Congress, 1st Session, 22-23 August 1995. A distressingly accurate account of the secret briefing we provided to President Clinton can be found in Andrew Cockburn and Leslie Cockburn, *One-Point Safe* (New York: Anchor Books/Doubleday, 1997). Much of the rest of that book, however, is filled with inaccuracies.

[26] Graham T. Allison et al., *Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nulcear Weapons and Fissile Material* (Cambridge, MA: MIT Press, 1996).

[27] See, for example, William C. Potter, "Before the Deluge? Assessing the Threat of Nuclear Leakage from the Post-Soviet States," *Arms Control Today* October (1995); Frank von Hippel, "Fissile Material Security in the Post-Cold War World," *Physics Today* 48, no. 6 (June 1995); Thomas B. Cochran, "Safety and Control of Nuclear Materials and Nuclear Weapons," paper presented at Economic and Social Development in the Former Soviet Union and the Problem of Nuclear Disarmament, Como, Italy, 3-4 July 1995.

continuing literature addressing it). The book *America's Achilles Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack,*[28] also produced at the Belfer Center, was an early exemplar of this trend, as were Gavin Cameron's *Nuclear Terrorism: A Threat Assessment for the 21st Century,*[29] Jessica Stern's *The Ultimate Terrorists,*[30] and work by Bruce Hoffman and others.[31]

Many of these analyses made the point that while U.S. and international policy has long been based on the premise that states can be deterred from using nuclear weapons by the threat of retaliation, at least some terrorist groups may not be restrained either by fear of retaliation or by the developing global norm against the use of nuclear weapons (which have not been used in anger since 1945). As will be discussed in Chapter 2, many terrorist groups are not remotely interested in the nuclear level of violence, for these and other reasons; but a fraction of terrorist groups, with global ambitions or dreams of apocalypse, have actively attempted to get nuclear weapons, and the risk that the probability that they would actually use a nuclear bomb if they could get one is far higher than the probability that a nuclear-armed state would do so.[32]

Concern about nuclear theft and terrorism increased substantially after the 9/11 attacks, when there were a number of important analyses of nuclear security (not only in the former Soviet Union but around the world) and of al Qaeda's attempts to acquire nuclear weapons. These included, for example, a series of reports by the present author and others associated with the Managing the Atom project at the Belfer Center, including the 2002 *Securing Nuclear Weapons and Materials: Seven Steps for Immediate Action* (which laid out explicitly the need for rapid action to secure nuclear stockpiles not only in the former Soviet Union, but in countries around the world); 2003's *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (which again highlighted the global nature of the threat and the actions needed to address it, described terrorist efforts to acquire nuclear weapons, and laid out a step-by-step "terrorist pathway to the bomb" and actions governments could take to block each of the steps on the pathway); 2004's *Securing the Bomb: An Agenda for Action* (which provided a more detailed set of arguments against a series of myths about terrorists and nuclear weapons that have led policymakers to downplay the nuclear terrorism danger); 2005's *Securing the Bomb 2005: The New Global Imperatives* (which provided an updated threat assessment and the latest measures of progress in reducing the threat); and 2006's *Securing the Bomb 2006* (which provided a detailed set of recommendations for a

---

[28] Richard A. Falkenrath, Robert Newman, and Bradley Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, MA: MIT Press, 1998).
[29] Gavin Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (New York: St. Martins Press, 1999).
[30] Jessica Stern, *The Ultimate Terrorists* (Cambridge, Mass.: Harvard University Press, 1999).
[31] See, for example, Bruce Hoffman, "Terrorism and WMD: Some Preliminary Hypotheses," *Nonproliferation Review* 4, no. 3 (1997; available at http://cns.miis.edu/pubs/npr/vol04/43/hoffma43.pdf as of 2 January 2007).
[32] See, for example, discussions in Falkenrath, Newman, and Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*; Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century.*

global coalition to combat nuclear terrorism and steps that could be taken to increase the sense of urgency about the threat in countries around the world).[33]

Other notable recent contributions in this category include Graham Allison's 2004 book, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*;[34] the work by Charles Ferguson, William Potter and others at Monterey, *The Four Faces of Nuclear Terrorism*;[35] the pioneering work by David Albright and others analyzing al Qaeda's nuclear efforts;[36] studies by Frank von Hippel and others at Princeton and Stanford;[37] analyses by Peter Zimmerman and colleagues;[38] and a few European studies that have expressed a similar view.[39] A notable

---

[33] Matthew Bunn, John Holdren, and Anthony Wier, *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/securing_nuclear_weapons_and_materials_May2002.pdf as of 2 January 2007); Matthew Bunn, Anthony Wier, and John Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/cnwm.pdf as of 2 January 2007); Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007); Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 2 January 2007); Bunn and Wier, *Securing the Bomb 2006*.

[34] Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*.

[35] Charles D. Ferguson and William C. Potter, with Amy Sands, Leonard S. Spector, and Fred L. Wehling, *The Four Faces of Nuclear Terrorism*, ed. Amy Sands, Leonard S. Spector, and Fred L. Wehling (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004; available at http://www.nti.org/c_press/analysis_4faces.pdf as of 2 January 2007).

[36] David Albright, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents," *Nautilus Institute Special Forum* 47 (2002; available at http://www.nautilus.org/archives/fora/Special-Policy-Forum/47_Albright.html as of 2 January 2007); David Albright, Kathryn Buehler, and Holly Higgins, "Bin Laden and the Bomb," *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.isis-online.org/publications/terrorism/binladenandbomb.pdf as of 2 January 2007), pp. 23-24; David Albright and Holly Higgins, "A Bomb for the Ummah," *Bulletin of the Atomic Scientists* 59, no. 2 (March/April 2003; available at http://www.thebulletin.org/issues/2003/ma03/ma03albright.html as of 2 January 2007), pp. 49-55.

[37] See, for example, Christopher F. Chyba, Hal Feiveson, and Frank Von Hippel, *Preventing Nuclear Proliferation and Terrorism: Essential Steps to Reduce the Availability of Nuclear-Explosive Materials* (Palo Alto, Cal.: Center for International Security and Cooperation, Stanford Institute for International Studies, Stanford University and Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2005; available at http://iis-db.stanford.edu/pubs/20855/Prvnt_Nuc_Prlf_and_Nuc_Trror_2005-0407.pdf as of 2 January 2007).

[38] Anna M. Pluta and Peter D. Zimmerman, "Nuclear Terrorism: A Disheartening Dissent," *Survival* 48, no. 2 (Summer 2006); Peter D. Zimmerman and Jeffrey G. Lewis, "The Bomb in the Backyard," *Foreign Policy*, no. 157 (November/December 2006), pp. 32-39.

[39] See, for example, Jeffrey Boutwell, Francesco Calogero, and Jack Harris, "Nuclear Terrorism: The Danger of Highly Enriched Uranium," *Pugwash Issue Briefs* 2, no. 1 (September 2002; available at http://www.pugwash.org/publication/pb/sept2002.pdf as of 3 April 2006); Morten Bremer Maerli, *Crude Nukes on the Loose? Preventing Nuclear Terrorism by Means of Optimum Nuclear Husbandry, Transparency, and Non-Intrusive Fissile Material Verification* (Oslo: Unipub AS, 2004; available at http://www.nupi.no/IPS/filestore/MBM_dissertation2004.pdf as of 4 April 2006); Frank Barnaby, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction* (New York: Nation Books, 2004); Annette Schaper, "Nuclear Terrorism:

analysis by Michael Levi is forthcoming.[40] There has also been a wide range of skeptical analyses downplaying the risk over this period.[41]

There are many varieties of terrorism and of terrorist groups, with a wide range of motivations and methods.[42] This dissertation is not the place for a complete analysis of the causes and risks of terrorism generally and how to reduce them; nor is it the place to debate the age-old question of who is a terrorist and who is a freedom fighter. Most terrrorist groups are focused on local issues and have modest capabilities; as a result, most terrorist groups have little potential for escalating to the nuclear level of violence. In this dissertation, I simply assume that use or threatened use of a nuclear bomb by a sub-national group constitutes nuclear terrorism, and that any sub-national group that would engage in such activity can fairly be described as terrorists.

This literature qualitatively assessing the nuclear terrorism threat is already rich. In this dissertation, I draw on this literature and new research to provide an integrated discussion of the key issues in a single chapter, with an updated assessment of the threat as it has evolved in recent years.

By contrast, there have been only a modest number of attempts to model mathematically the global risks of nuclear theft and terrorism, perhaps because of the immense uncertainties in doing so. One model currently used to estimate terrorism risks for the insurance industry includes nuclear terrorism among many other terrorist threats to insured properties; but because it is a commercial product, none of its methods and assumptions have been made publicly available.[43] Some previous mathematical models of nuclear terrorist risks assumed that each facility with potential bomb material had a fixed probability of theft, so that the total probability increased linearly with deployment of more facilities,[44] or that the risk posed by each category of nuclear material was proportional to the

---

Risk Analysis after 9/11," *Disarmament Forum*, no. 2 (2003; available at http://www.unidir.ch/pdf/articles/pdf-art1907.pdf as of 4 April 2006).

[40] Michael Levi, *On Nuclear Terrorism* (Cambridge, Mass.: Harvard University Press, 2007).

[41] See, for example, Kamp, "Nuclear Terrorism Is Not the Core Problem"; Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy* (Fall 1998; available at http://jya.com/superterror.htm as of 4 April 2006); Robin M. Frost, "Nuclear Terrorism after 9/11," *Adelphi Papers*, no. 378 (2005).

[42] For two notable recent overviews, see Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006); Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

[43] For a general overview of the conceptual approach used in this model, developed by Gordon Woo and colleagues at the firm Risk Management Solutions, see Gordon Woo, "Quantitative Terrorism Risk Assessment," *Journal of Risk Finance* 4, no. 1 (October 2002; available at http://www.rms.com/NewsPress/Quantitative_Terrorism_Risk_Assessment.pdf as of 22 May 2006). Somewhat more detail on some of the terrorist scenarios included in the model can be found in Henry H. Willis et al., *Estimating Terrorism Risk* (Santa Monica, Cal.: RAND, 2005; available at http://www.rand.org/pubs/monographs/2005/RAND_MG388.pdf as of 6 May 2006).

[44] Roger E. Avedon, "On the Future of Civilian Plutonium: An Assessment of Technological Impediments to Nuclear Terrorism and Proliferation" (Ph.D. dissertation, Engineering Economic Systems and Operations Research, Stanford, 1997).

quantity of material in that category.[45] The model presented here is simpler in its mathematics than some previous models, but more realistic in its assumptions. It assumes that there are a limited number of plausible nuclear terrorist groups who undertake a limited number of attempts to acquire nuclear weapons or materials. This means that the relationship between the risk and the quantity of facilities or materials is much less direct than in previous models. The model presented here is more closely tied to past experience with the different parameters than previous models and is focused specifically on its use for analyzing the effectiveness of policy responses along the entire chain from the formation of groups capable enough to contemplate nuclear terrorism to managing the consequences of a terrorist nuclear explosion.

Identifying the Highest-Priority Risks of Nuclear Theft

The literature on this subject is thin. Previous authors have not attempted to lay out systematic approaches to considering whether a facility in one country poses a higher or lower risk than a different type of facility in another.

Indeed, it is a remarkable fact that no government or non-government study has yet undertaken an in-depth effort to assess where the greatest risks of nuclear theft are worldwide. (The first introduction to the general approach presented in this dissertation appeared in 2004's *Securing the Bomb: An Agenda for Action*, mentioned above.) No database exists anywhere in the world, classified or unclassified, that includes all the essential elements of such an assessment: estimates of all the facilities worldwide where nuclear weapons or weapons-usable nuclear material exist; how much material, of what types, is at these facilities; the quality of the security and accounting arrangements at these facilities; and the levels of terrorist and criminal threats that these facilities face. There are, however, a variety of databases, at the International Atomic Energy Agency (IAEA), in the U.S. government, and elsewhere, that contain pieces of this information. The U.S. Department of Energy has come closest to putting together an integrated assessment, with a list of the facilities believed to contain weapons-usable nuclear material worldwide, estimates of the amount at each facility, and simple high-medium-low ratings for the quality of the material and the security level at each site.[46] The IAEA has detailed data on how much nuclear material, of what types, exists at all safeguarded facilities around the world – but this does not include data on security arrangements or on threats, and it excludes nearly all facilities in nuclear weapon states, where most of the world's potential nuclear bomb material resides. Thus, laying out this systematic approach to identifying the highest-priority facilities – and then using what publicly available data exist to take a first cut at applying the method to a few countries as examples – is a major contribution of this dissertation.

For decades, governments around the world *have* considered how the factors of material quantity and material quality affect the risks that theft of these materials would pose

---

[45] See Edwin Zebrowski, "Analysis of Risks of Diversion of Plutonium or Highly Enriched Uranium," reproduced in Committee on Science, Space, and Technology, *Conversion of Research and Test Reactors to Low-Enriched Uranium (LEU) Fuel*, U.S. Congress, House of Representatives, 98th Congress, 2nd Session, 25 September 1984, pp. 60-74.

[46] Interview with DOE official, November 2005.

and on that basis have made decisions about what levels of security and safeguards to apply to different types and quantities of nuclear material. In the Convention on Physical Protection of Nuclear Material, for example, and in the IAEA recommendations on physical protection, there are tables that categorize nuclear material in three different categories of risk, with Category I requiring the most intensive security and accounting measures.[47] Any stockpile containing more than 2 kilograms of unirradiated plutonium, or more than 5 kilograms of uranium-235 contained in uranium enriched to 20% or more, is considered Category I material in this approach.

Many countries have based their own domestic approaches to categorization on these international standards, but others (including both the United States and Russia) have implemented somewhat different approaches, which reflect a different assessment of the risks posed by particular types of nuclear materials. In the U.S. Department of Energy system, for example, a wide range of materials containing large amounts of plutonium and HEU that terrorists might well be able to process for use in a nuclear weapon are placed in a category requiring only modest security, because they contain less than 10 percent plutonium or U-235 by weight. This would include, for example, fresh plutonium-uranium mixed oxide (MOX) fuels and HEU research reactor fuels. There is an extensive literature, much of it from the U.S. nuclear weapons laboratories, describing arguments for and against the quantity and quality thresholds in the international standards and the standards used in the United States, but much of that literature is classified or otherwise unavailable. Fortunately, for this dissertation, I have been able to acquire a number of the underlying source documents relating to these issues from within the U.S. government and have been able to acquire more information through interviews.[48] Substantial modifications to the U.S. categorization approach, bringing it more closely in line with international approaches, are among the major recommendations of that chapter of this dissertation.

Some approaches have also integrated evaluations of the effectiveness of security at a site with assessments of the quantity and quality of the material there, into an overall assessment of risk. At the facilities managed by the U.S. Department of Energy, for example, security rules do require comparative assessments of overall nuclear theft risk, based on the types and quantities of material present and the estimated effectiveness of each facility's

---

[47] International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected) (Vienna: IAEA, 1999; available at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html as of 22 December 2006); International Atomic Energy Agency, *The Convention on Physical Protection of Nuclear Material*, INFCIRC/274/Rev. 1 (Vienna: IAEA, 1980; available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml as of 29 July 2005).

[48] In particular, although various orders relating to nuclear security and accounting have been issued much more recently, as of 2006 the document that still provided the underlying basis for determining which materials should be put in which category within the U.S. Department of Energy system was U.S. Department of Energy, *Guide to Implementation of DOE 5633.3b, "Control and Accountability of Nuclear Materials"* (Washington, D.C.: DOE, 1995).

security and accounting systems.[49] These estimates rely on systematic vulnerability assessment methodologies originally developed in the 1970s and refined substantially since then. These assessments are based on a conceptual approach similar to that which will be outlined in this dissertation, but they are based on one overall threat estimate (the "design basis threat") for the entire United States. No attempt has been made to assess threats as a probabilistic spectrum of different possibilities, or to assess threats comparatively on a global basis to determine where the highest priorities are for improving nuclear security to keep nuclear material out of terrorist hands. The probabilistic approach to assessing threats is another major contribution of this dissertation.

Of course, for such a global assessment, information about the level of security at different sites is critical. The data on this subject that is publicly available is very limited, as nearly every country regards the specifics of its nuclear security arrangements as closely guarded secrets. The United States openly publishes more about its nuclear security arrangements than any other country and has a particularly active group of non-government organizations and reporters regularly finding and publishing additional information which had not necessarily been intended for public release.[50] While some specifics remain classified, by combining published sources with interviews it is possible to gain a reasonably detailed understanding of the state of nuclear security at many U.S. nuclear facilities.

In the former Soviet Union, the secrecy surrounding nuclear security is much more extensive, but after more than a decade of international cooperation to improve security and accounting arrangements, U.S. and other international experts have learned a great deal about some aspects of nuclear security. A considerable amount of important information has been openly published by either U.S. or Russian participants in these cooperative efforts,[51] and by combining this information with interviews, a reasonable overview of the situation can be developed, though significant gaps in the picture remain.[52] Publicly available information on

---

[49] For a brief discussion of these assessments, see, for example,U.S. Congress, Government Accountability Office, *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat* (GAO, 200423 December 2006).

[50] For some recent examples, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Security at Risk* (Washington, D.C.: POGO, 2001; available at http://www.pogo.org/p/environment/eo-011003-nuclear.html as of 4 December 2006); Project on Government Oversight, *Nuclear Power Plant Security: Voices from inside the Fences* (Washington D.C.: POGO, 2002; available at http://www.pogo.org/p/environment/eo-020901-nukepower.html as of 2 January 2007); Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006); Daniel Hirsch, David Lochbaum, and Edwin Lyman, "The Nrc's Dirty Little Secret," *Bulletin of the Atomic Scientists* (May/June 2003; available at http://www.thebulletin.org/article.php?art_ofn=mj03hirsch as of 5 February 2006), pp. 44-51; Daniel Hirsch, "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.thebulletin.org/article.php?art_ofn=jf02hirsch as of 8 January 2007), pp. 38-44.

[51] See, for example, the papers included in the proceedings of the annual meetings of the Institute for Nuclear Materials Management, from 1997 to the present.

[52] For an example of such overviews, see Matthew Bunn, "The Threat in Russia and the Newly Independent States," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2006; available at http://www.nti.org/e_research/cnwm/threat/russia.asp as of 2 January 2007).

practices in most other countries is less detailed, but many countries have made public presentations about their nuclear security approaches at a series of international conferences and workshops in recent years, and these, too, can be supplemented with interviews.[53]

Finally, there is the problem of assessing the threat levels in different countries. Threats that could lead to nuclear theft include terrorist activity, violent and organized crime activity, and government corruption. Low pay and morale among nuclear workers, along with insufficient funding for nuclear facilities, could contribute to the threat of insider theft. This dissertation relies on published indices of terrorist activity, crime, and corruption (some of which are prepared to help businesses assess the crime and terrorism risks they face in different countries, which are closely related to nuclear theft risks) as indicators of the level of theft threat in different countries;[54] in the absence of published data on pay for nuclear workers and guards, this dissertation uses per capita gross domestic product (adjusted for purchasing power parity) as a rough proxy for likely pay scales and the levels of resources likely to be available to fund nuclear facilities.

Understanding the Global Nuclear Security System – and Assessing Tools for Change

Over the years, there have been a number of assessments of particular programs at particular times, generally focused on how to overcome specific issues within that program at that moment. [55] Some analyses have sought to review the record of one particular policy tool

---

[53] See, for example, Lawrence Livermore National Laboratory, *Comparative Analysis of Approaches to Protection of Fissile Materials: Proceedings of a Workshop at Stanford University, 28-30 July 1997* (Livermore, Cal.: LLNL, 1997); International Atomic Energy Agency, ed., *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations, Vienna, 10-14 November* (Vienna: IAEA, 1997); International Atomic Energy Agency, *Security of Material: Measures to Prevent, Intercept, and Respond to Illicit Uses of Nuclear Material and Radioactive Sources: Proceedings of a Conference in Stockholm, Sweden, 7-11 May 2001* (Vienna: IAEA, 2001); International Atomic Energy Agency, *Proceedings of the Symposium on International Safeguards: Verification and Nuclear Material Security, Vienna, 29 October-2 November 2001* (Vienna: IAEA, 2001); Fritz Steinhausler, ed., *Proceedings of Strengthening Global Practices for Protecting Nuclear Material: Eu-High Level Scientific International Conference on Physical Protection, Salzburg, Austria, 8-13 September* (Salzburg, Austria: University of Salzburg, 2002; available at http://www.numat.at/list%20of%20papers/gesamtproceedings.pdf as of 4 December 2006).

[54] See, for example, Transparency International, *Corruption Perceptions Index 2004* (Berlin: TI, 2004; available at http://www.transparency.org/content/download/1532/7971/file/media_pack_en.pdf as of 16 November 2006); Transparency International, *Report on the Transparency International Global Corruption Barometer 2004* (Berlin: TI, 2004; available at http://www.transparency.org/content/download/1558/8065/file/barometer_report_8_12_2004.pdf as of 13 December 2006); Guy Dunn, *WMRC Global Terrorism Index 2003/2004* (London: World Markets Research Centre, 2003).

[55] Many of these programs, for example, have been assessed at one time or another by the U.S. Government Accountability Office, the U.S. National Academy of Sciences, or other official or semi-official groups. As two recent examples, see U.S. Congress, General Accounting Office, *Weapons of Mass Destruction: Additional Russian Cooperation Needed to Facilitate U.S. Efforts to Improve Security at Russian Sites*, GAO-03-482 (Washington, D.C.: GAO, 2003; available at http://www.gao.gov/new.items/d03482.pdf as of 4 March 2005); U.S Committee on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, National Research Council, and Russian Committee on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, Russian Academy of Sciences, *Strengthening U.S.-Russian Cooperation on Nuclear Nonproliferation* (Washington, D.C.: National Academy Press, 2005; available at http://fermat.nap.edu/catalog/11302.html as of 2

– from technical cooperation to install modern security and accounting systems at particular sites, to efforts to negotiate more stringent global nuclear security standards – and to draw lessons for making that tool more effective in the future.[56] But no previous analysis has attempted to compare the record of different policy tools for improving nuclear security using a consistent set of criteria, to learn lessons about which tools are most effective under which circumstances. Moreover, there has been no previous effort to describe and assess the myriad approaches to nuclear security that exist worldwide and their interconnections as a complex global system, to help clarify how the performance of that system might be improved. Thus, another major contribution of this dissertation is to provide an analysis of the structure of the global nuclear security system and to combine that understanding with the history of past efforts to improve nuclear security, generating at least preliminary judgments about which policy tools are likely to be most effective in the future.

Boundaries and Limitations of the Study

This dissertation does not cover all the different possible types of nuclear terrorism, from dispersal of radioactive material in a so-called "dirty bomb," to sabotage of a major

---

January 2007). There is also a large literature of academic and non-government-organization assessments of particular programs in these areas. See, for example, the assessments of dozens of these programs (with annotated links to the best information on them available on the internet) in Matthew Bunn and Anthony Wier, *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative; available at http://www.nti.org/securingthebomb as of 3 April 2006). For further examples, in addition to the annual *Securing the Bomb* series cited above, see James Clay Moltz, "Special Report: Assessing U.S. Nonproliferation Assistance in the NIS," *Nonproliferation Review* 7, no. 1 (Spring 2000 2000; available at http://cns.miis.edu/pubs/npr/vol07/71toc.htm as of 4 December 2006); John M. Shields and William C. Potter, *Dismantling the Cold War: U.S. And NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program* (Cambridge, MA: MIT Press, 1997); Matthew Bunn, *The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material* (Washington, D.C.: Managing the Atom Project, Harvard University, and Non-Proliferation Project, Carnegie Endowment for International Peace, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/FullNextWave.pdf as of 2 January 2007); Matthew Bunn and John P. Holdren, "Managing Military Uranium and Plutonium in the United States and the Former Soviet Union," *Annual Review of Energy & the Environment* 22, no. 1 (1997; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mmup.pdf as of 6 February 2006).

[56] For analyses of lessons learned from U.S.-Russian technical cooperation to install security upgrades, see, for example, Oleg Bukharin, Matthew Bunn, and Kenneth N. Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union* (Washington, D.C.: Russian American Nuclear Security Advisory Council, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mpca2000.pdf as of 2 January 2007); Caitlin Talmadge, "Striking a Balance: The Lessons of U.S.-Russian Materials Security Cooperation," *Nonproliferation Review* 12, no. 1 (March 2005; available at http://cns.miis.edu/pubs/npr/vol12/121/121talmadge.pdf as of 2 November 2005); Matthew Bunn, "Cooperation to Secure Nuclear Stockpiles: A Case of Constrained Innovation," *Innovations* 1, no. 1 (2006; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/INNOV0101_CooperationtoSecureNuclearStockpiles.pdf as of 4 April 2006). For analyses of efforts to impose tighter international standards for nuclear security, see, for example, Bonnie Jenkins, "Establishing International Standards for Physical Protection of Nuclear Material," *Nonproliferation Review* 5, no. 3 (Spring-Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/jenkin53.pdf as of 19 July 2005); George Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," *Nonproliferation Review* 7, no. 2 (Summer 2000; available at http://cns.miis.edu/pubs/npr/vol07/72/72bunn.pdf as of 2 January 2007).

nuclear facility, to simple hoaxes.[57] These are real dangers that also have to be addressed; but for reasons of time and resources, I have chosen to focus here only on preventing terrorists from accomplishing the most devastating form of nuclear terrorism, the use of an actual nuclear explosive. Similarly, this study does not attempt to provide a comprehensive analysis of everything that ought to be done to reduce the danger of nuclear weapons terrorism – from offensive action against terrorist groups with potential nuclear ambitions to improved ability to respond and recover in the event of such an attack – though the full spectrum of such policies can be assessed using the mathematical model presented here, and the dissertation does present some initial thoughts about initial actions that might be possible at each point in the terrorist pathway to the bomb.[58] Nor does this analysis cover everything that should be done to improve the management of nuclear weapons and materials around the world – from comprehensive declaration and monitoring of such stockpiles, to ending further production of such dangerous commodities, to reducing the excess stockpiles that already exist.[59] Instead, it focuses primarily on ensuring that these stockpiles are effectively secured and accounted for. This dissertation will make the case that this is the single point on the terrorist pathway to the bomb where policy measures can accomplish the biggest reductions in the overall risk of nuclear terrorism.

The limitations of available data and resources inevitably imposed significant constraints on this study. As already noted, the specific measures taken to secure nuclear stockpiles and facilities are closely guarded secrets in most countries of the world; hence, data on the specific security measures in place at different facilities is spotty at best, available primarily from actual visits to such facilities and discussions with others who have participated in such visits. The number of nuclear facilities (and other types of guarded facilities) I could visit during the period of the study was limited both by time and resources and by the requirement to get official permissions for such visits, which are generally not forthcoming for particularly sensitive nuclear facilities. (In Russia, in particular, facilities that were quite open to visits by foreign academics in 1992-2000 are now generally off-limits to people not participating in officially sponsored nuclear cooperation.) Nevertheless, after more than a decade of work on these issues, I am confident that I have compiled sufficient information to make a contribution to clarifying the key issues the world faces in attempting

---

[57] For a recent account that includes these other types of nuclear terrorism, see Ferguson and Potter, *The Four Faces of Nuclear Terrorism.*

[58] For an earlier attempt to describe each step terrorists would have to take to get to the point of being able to detonate a nuclear bomb in a major city and the steps that governments could take to try to block these steps (dubbed "Blocking the Terrorist Pathway to the Bomb"), see Bunn, Wier, and Holdren, *Controlling Nuclear Warheads and Materials*, pp. 20-32.

[59] For accounts of the status of these other issues and programs to address them, see Bunn and Wier, *Nuclear Threat Initiative Research Library: Securing the Bomb.* See also International Panel on Fissile Materials, *Global Fissile Material 2006: Report of the International Panel on Fissile Materials* (Princeton, N.J.: Program on Science and Global Security, Princeton University, 2006; available at http://www.fissilematerials.org/ipfm/site_down/ipfmreport06.pdf as of 24 January 2007). That report is the first of an expected annual series. For a very recent account of potential regimes for monitoring total stockpiles of nuclear warheads and materials, see U.S. National Academy of Sciences, Committee on International Security and Arms Control, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials* (Washington, D.C.: National Academy Press, 2005; available at http://books.nap.edu/catalog/11265.html as of 8 August 2005).

to ensure that all nuclear stockpiles are effectively secured and accounted for. More information on certain key points would surely change the picture painted here at the margins, but the broad outlines would, I believe, remain the same.

Because of limitations of time and space, this dissertation provides only a brief first cut at describing the history of the development of the global nuclear security system and the factors that caused security upgrades to be undertaken in particular countries and particular times (and that constrained those improvements from going farther than they did). This is an area of ongoing research. For similar reasons, this dissertation does not go into great depth on two areas that are critical to the future of nuclear security efforts: how to ensure that heightened nuclear security measures will be sustained over time, and how to select, train, and motivate staff to ensure that they give security the priority it deserves, forging an effective "security culture." Excellent recent treatments of both sustainability and security culture are available,[60] but there is considerably more research to be done.

This study is inevitably from an American perspective, and it must be acknowledged that the perspective in the United States – which probably spends more on nuclear security and has more stringent rules for securing its stockpiles than any other country in the world and has probably the highest levels in the world of both public and elite concern over the possibility of terrorist use of nuclear explosives – is quite different from the perspective in many other countries.

Definitions

Only a few terms used in this dissertation require defining up-front:

Nuclear security and accounting. When I use the phrase *nuclear security* or *security for nuclear stockpiles,* I am usually referring to the whole complex of measures designed to reduce the probability of theft of nuclear weapons or materials from a particular facility or transport leg. Most important among these are the measures often referred to as *physical protection*, such as fences, intrusion detectors, guard forces, walls, vaults, and the like, which are intended to detect, delay, and defeat actions by adversaries to steal nuclear weapons or materials. Nuclear security, as used here, also includes what is sometimes known as *personnel reliability* and *access control* measures – steps to limit access to particular facilities or areas to individuals whose trustworthiness has been reviewed and who have been granted appropriate clearances, and to continuously review the trustworthiness of cleared personnel. Nuclear security, as used here, can also include those measures of *material control and accounting* (MC&A) that are most relevant to preventing theft – though on occasion I also use the phrase *nuclear security and accounting,* in contexts where the inclusion of the accounting measures is especially important. MC&A includes approaches to accurately measuring and

[60] See, for example, Igor Khripunov and James Holmes, eds., *Nuclear Security Culture: The Case of Russia* (Athens, Georgia: Center for International Trade and Security, The University of Georgia, 2004; available at http://www.uga.edu/cits/documents/pdf/Security%20Culture%20Report%2020041118.pdf as of 18 February 2005); Committee on Indigenization of Programs to Prevent Leakage of Plutonium and Highly Enriched Uranium from Russian Facilities, Office for Central Europe and Eurasia, National Research Council, *Strengthening Long-Term Nuclear Security: Protecting Weapon-Usable Material in Russia* (Washington, D.C.: National Academy Press, 2005; available at http://fermat.nap.edu/catalog/11377.html as of 4 April 2006).

keeping account of nuclear materials on-hand, so that any substantial removal of nuclear material would be noticed. It also includes material control measures, such as tags, seals, security cameras, and the like, intended to ensure that any removal or unauthorized access would be detected, ideally in real time. Combined, the whole system of physical protection and MC&A technologies is referred to as *material protection, control, and accounting* (MPC&A). While police, intelligence, and related measures play an important role in reducing the probability that large conspiracies to steal nuclear material can carry out their plans without being detected and disrupted, and complement the security and accounting measures taken at individual sites, the activities involved in police and intelligence measures are quite different and I treat them separately in this dissertation, rather than including them in the general term "nuclear security."

Weapons-usable nuclear material. In this dissertation, I use the term *weapons-usable nuclear material* to refer to material that contains material capable of supporting the fast-critical nuclear chain reaction required for a nuclear explosive without further enrichment, in forms that are not so radioactive that they would require complex remote-handling equipment to process the material into a form usable in a nuclear bomb. Here, the term has essentially the same meaning as the International Atomic Energy Agency (IAEA) term *unirradiated direct-use nuclear material.*[61] The principal materials concerned are HEU (defined both in the United States and internationally as uranium containing 20 percent or more the isotope U-235),[62] and plutonium separated from fission products (in essentially any mix of isotopes except those with extremely high concentrations of the isotope Pu-238).[63] *Weapons-grade* material refers to plutonium or HEU that has the mix of isotopes that weapon designers prefer, typically more than 90% U-235 in the case of HEU, or more than 90% Pu-239 in the case of plutonium; a much wider range of mixtures, however, are weapons-usable, even with no more sophistication than needed to make a bomb from weapon-grade material, and therefore of concern in addressing the risk of nuclear terrorism.[64] U-233 is also recognized as

---

[61] The IAEA defines direct-use material as HEU, plutonium containing less than 80% Pu-238, and U-233. Unirradiated direct-use material is material which "does not contain substantial amounts of fission products" and hence "would require less time and effort to be converted to components of nuclear explosive devices." International Atomic Energy Agency, *IAEA Safeguards Glossary* (Vienna: IAEA, 2001; available at http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/Start.pdf as of 19 July 2005), p. 33. For purposes of physical protection against theft, the IAEA defines any material emitting more than 100 rad/hr at one meter as "irradiated," and hence requiring less stringent security. International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*. As will be discussed in Chapter 4, the 100 rad/hr at 1 meter standard (also used in U.S. regulations and in many national regulations around the world) should be reconsidered in light of current, post-9/11 threats.

[62] International Atomic Energy Agency, *IAEA Safeguards Glossary*, p. 32. In principle, nuclear explosives can be fabricated from uranium at enrichments below 20 percent, but the amounts required are quite large. See Chapter 4 for a more detailed discussion of how the isotopic content of uranium affects the ease or difficulty of using it in nuclear explosives.

[63] In IAEA practice, all plutonium except plutonium including 80% or more of Pu-238 requires safeguards. International Atomic Energy Agency, *IAEA Safeguards Glossary*, p. 17. Chapter 4 provides a more detailed discussion of how the isotopic content of plutonium affects the ease or difficulty of using it in nuclear explosives.

[64] See Chapter 4 for an extended discussion of the barriers to making nuclear explosives posed by different mixes of uranium and plutonium isotopes.

weapons-usable in international practice, and there are a range of other isotopes which could be used to fabricate nuclear explosives.[65] Mixtures containing these materials that could be chemically separated without remote handling, such as uranium-plutonium mixed oxide (MOX) fuel, or uranium-aluminum research reactor fuel, are included in the term "weapons-usable nuclear material."

Nuclear weapons, nuclear bombs, and ***nuclear explosives.*** In this dissertation, I generally use the term *nuclear explosive* to refer to any device capable of generating a substantial nuclear blast. I usually use the term *nuclear weapons* to refer only to the relatively sophisticated nuclear explosives designed and built by states, generally intended to meet specified standards for yield, reliability, and safety, and sometimes intended to be small, light, and rugged enough to be launched on a ballistic missile or fired from a cannon. I use the term *nuclear bomb,* by contrast, to refer to the relatively crude kinds of nuclear explosive that a terrorist group might be able to devise, which would probably be large and heavy and have unknown yield and reliability.

Plan of the Study

Chapter 2 of this dissertation provides a qualitative assessment of the global risks of nuclear theft and terrorism, including:

- publicly available information concerning terrorist attempts to acquire nuclear weapons and materials (and, to a lesser extent, the efforts of selected states to acquire stolen nuclear materials for their weapons programs);
- the danger that terrorists could succeed in getting a stolen nuclear bomb or the plutonium or HEU needed to make one;
- the size, distribution, and rates of change of global nuclear stockpiles; and
- current approaches to securing and accounting for these stockpiles and how they vary from country to country.

This chapter also provides the essential background material supporting the remainder of the dissertation

Chapter 3 introduces the mathematical model of the global risk of nuclear terrorism, assessing each of the parameters of the model in detail. Chapter 4 then develops and applies the risk-based framework for identifying and prioritizing those nuclear facilities posing the highest risks. Chapter 5 analyzes the complex global system for securing nuclear stockpiles and assesses the record of different policy tools for improving the performance of this system. Finally, Chapter 6 offers conclusions and recommendations.

The single most important factor that has to change if high and lasting standards of security for the world's nuclear stockpiles are to be achieved is that world leaders – beginning, but not limited to, the presidents of the United States and Russia – will have to develop a sense of urgency and decide to devote themselves to getting this job done. This

[65] See Chapter 4 for a discussion of these other potentially weapons-usable isotopes.

dissertation, however, is not intended primarily as a call to action – other publications have served that purpose.[66] Rather, this dissertation is intended to explore what the experience gained so far suggests about what these leaders should do, if and when they decide to take further action.

[66] See, for example, Bunn and Wier, *Securing the Bomb 2005*; Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*.

2. The Global Threat of Nuclear Theft and Terrorism: A Qualitative Assessment

This chapter describes the current global threat of nuclear theft and nuclear terrorism. The facts that frame this danger, each of which will be discussed in turn, are stark:

- Terrorist groups and hostile states are actively seeking stolen nuclear weapons and materials and actively seeking to recruit nuclear expertise.
- Making at least a crude nuclear bomb is potentially within the capability of a capable and well-organized terrorist group, if they could get the needed nuclear material. Getting such material could also shave years off the time required for a hostile state to get a nuclear weapon – and make the remaining activities needed to do so very difficult to detect.
- Tens of thousands of nuclear weapons and enough weapons-usable nuclear material to make hundreds of thousands more exist in the world. These stockpiles are located in hundreds of buildings in dozens of countries.
- Security and accounting arrangements for these nuclear stockpiles range from excellent to appalling, with no binding global security standards in place. Weapons-usable nuclear material that is not sufficiently secure to protect against the threats that terrorists and criminals have proved they can pose exists in dozens of countries around the world.
- As a result of these conditions, a substantial number of incidents of actual theft of weapons-usable nuclear material have occurred.

There is no convincing evidence, however, that any terrorist group or proliferating state has yet received a stolen nuclear weapon or stolen weapons-usable nuclear material. Indeed, both al Qaeda and the Japanese cult Aum Shinrikyo, the two terrorist groups that have made the most substantial efforts to acquire nuclear weapons to date, have encountered a variety of difficulties, demonstrating that nuclear weapons and the materials and expertise needed to make them are difficult to acquire, even for large and well-financed terrorist groups with ample technical resources.

The Demand for Black-Market Nuclear Material and Expertise

None of the confirmed cases of seizures of stolen nuclear material includes clear evidence of a particular buyer – whether a state seeking nuclear weapons or a terrorist group.[1]

[1] This section is largely drawn from Matthew Bunn and Anthony Wier, with Joshua Friedman, "The Demand for Black Market Fissile Material," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/cnwm/threat/demand.asp as of 2 January 2007). On the lack of clear connections to buyers in the known cases, see, for example, Rensselaer Lee, *Nuclear Smuggling and International Terrorism: Issues and Options for U.S. Policy*, RL31539 (Washington, D.C.: Congressional Research Service, 2002);

Nevertheless, there is significant evidence that both terrorist groups and states hostile to U.S. interests have sought stolen nuclear weapons or weapons-usable nuclear materials and have attempted to recruit nuclear-weapons expertise. Indeed, there are disturbing indications that demand for stolen nuclear weapons or materials may be becoming more focused and sophisticated and may be coming closer to overcoming the gap between buyers and potential sellers. These indications include:

- Incidents of terrorist teams carrying out reconnaissance at nuclear weapon storage sites and on nuclear weapon transport trains in Russia, whose locations and schedules are state secrets;[2]
- Reports that the 41 heavily armed terrorists who seized hundreds of hostages at a theater in Moscow in October 2002 considered seizing the Kurchatov Institute, a site with enough highly enriched uranium (HEU) for dozens of nuclear weapons;[3] and
- The 2003 criminal case involving a Russian businessman who was offering $750,000 for stolen weapon-grade plutonium for sale to a foreign client – and succeeded in making contact with residents of the closed city of Sarov, home of Russia's equivalent of Los Alamos, to try to close the deal.[4]

Rensselaer Lee, "Nuclear Smuggling: Patterns and Responses," *Parameters: U.S. Army War College Quarterly* (Spring 2003; available at http://carlisle-www.army.mil/usawc/Parameters/03spring/lee.pdf as of 5 December 2005).

[2] The incidents involving warhead sites were confirmed publicly by Lt. Gen. Igor Valynkin, commander of the 12th Main Directorate of the Russian Ministry of Defense (often known by its Russian acronym as the 12th GUMO), charged with guarding and managing Russia's nuclear weapons. See, for example, Pavel Koryashkin, "Russian Nuclear Ammunition Depots Well Protected – Official," *ITAR-TASS*, 25 October 2001; "Russia: Terror Groups Scoped Nuke Site," *Associated Press*, 25 October 2001. Valynkin has also brought up these incidents in private discussions with U.S. officials. (Interview with U.S. defense contractor expert, February 2004.) The incidents involving warhead transport trains were reported by the Russian state newspaper. See Vladimir Bogdanov, "Propusk K Beogolovkam Nashli U Terrorista (a Pass to Warheads Found on a Terrorist)," *Rossiskaya Gazeta*, 1 November 2002. (It is worth noting that the title of this article is unduly sensationalistic – the pass the title refers to would have entitled the Chechen nationalist who possessed it to access to the closed nuclear city of Lesnoy, site of a major nuclear weapon assembly and disassembly facility, but not to the facility itself. He had the pass because he had once lived in Lesnoy, when his father worked at the facility; that the pass was not revoked or retrieved when the father's employment came to an end clearly reflects a problem in management of such passes.)

[3] Bogdanov, "A Pass to Warheads Found on a Terrorist." Bogdanov attributes this information to sources in the Russian security services. By this account, the terrorists' idea was to seize a reactor and threaten to blow it up, rather than to seize HEU; the terrorists reportedly concluded that it would be easier to seize the less-well-defended theater.

[4] For summaries of Russian press reports on this case, see Matthew Bunn, "Anecdotes of Insecurity," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/threat/anecdote.asp as of 2 January 2007); "Plutonium Con Artists Sentenced in Russian Closed City of Sarov," *NIS Export Control Observer* (November 2003; available at http://cns.miis.edu/pubs/nisexcon/pdfs/ob_0311e.pdf as of 23 December 2006). See in particular "Russian Court Sentences Men for Weapons-Grade Plutonium Scam," trans. BBC Monitoring Service, *RIA Novosti*, 14 October 2003; "Russia: Criminals Indicted for Selling Mercury as Weapons-Grade Plutonium," trans. U.S. Department of Commerce, *Izvestiya*, 11 October 2003.

To organize the discussion of such incidents, this section focuses, as important recent examples of demand for stolen nuclear weapons or weapons-usable nuclear materials, on: (a) al Qaeda and the global jihadist movement it has spawned; (b) Aum Shinryikyo (now known as Aleph); (c) Chechen terrorist groups; (d) Iraq, prior to the overthrow of Saddam Hussein; and (e) Iran. This list of cases is not intended to cover the entire universe of possible recipients of stolen nuclear weapons and materials, but only to convince the reader that there are both terrorist groups and states that have actively sought these items.

Al Qaeda and the Global Jihadist Network

Most terrorist groups have no interest in threatening or committing large-scale nuclear destruction. Focused on local issues, seeking to become the governments of the areas now controlled by their enemies (and thus not wanting to destroy those areas), needing to build political support that might be undermined by the horror and wanton destruction of innocent life that would result from a nuclear attack, all but a few terrorist groups probably would not want to get and use a nuclear bomb even if they could readily do so.[5]

There are, however, a few dangerous exceptions that *do* seek to cause mass destruction and might be able to put together the capability to do so. Al Qaeda and the global jihadist network it has spawned are at the top of this list. On September 11, 2001, they permanently put to rest the complacent belief that those crazy enough to want to kill large numbers of people would be crazy enough to be unable to put together the means to do so. They are focused, not on a local battle for which the immense power of nuclear weapons might be seen as unnecessary, but on a global struggle, in which nuclear weapons might well be seen as essential instruments. Bin Laden and his al Qaeda terrorist network have made their own desire for nuclear weapons for use against the United States and its allies explicit, by both word and deed. Bin Laden has called the acquisition of weapons of mass destruction (WMD)

---

[5] For discussions, see, for example, Amy Sands, "The Nuclear Terrorists: Who, Why, and How Capable," in Charles D. Ferguson and William C. Potter, with Amy Sands, Leonard S. Spector, and Fred L. Wehling, *The Four Faces of Nuclear Terrorism*, ed. Amy Sands, Leonard S. Spector, and Fred L. Wehling (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004; available at http://www.nti.org/c_press/analysis_4faces.pdf as of 2 January 2007); Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004), pp. 19-42; Jessica Stern, *The Ultimate Terrorists* (Cambridge, Mass.: Harvard University Press, 1999); Richard A. Falkenrath, Robert Newman, and Bradley Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, MA: MIT Press, 1998); Bruce Hoffman, "Terrorism and WMD: Some Preliminary Hypotheses," *Nonproliferation Review* 4, no. 3 (1997; available at http://cns.miis.edu/pubs/npr/vol04/43/hoffma43.pdf as of 2 January 2007); Gavin Cameron, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (New York: St. Martins Press, 1999); Brian M. Jenkins, "Will Terrorists Go Nuclear? A Reappraisal," in *The Future of Terrorism: Violence in the New Millenium*, ed. Harvey W. Kushner (London: Sage, 1998).

a "religious duty."[6] Al Qaeda has been seeking to buy stolen nuclear weapons or nuclear material and to recruit nuclear expertise for more than a decade.[7]

Al Qaeda has gone to considerable lengths to justify to its supporters and audiences the use of mass violence, including the mass killing of innocent civilians, and they have explicitly set inflicting the maximum possible level of damage on the United States and its allies as one of their organizational goals. Intercepted al Qaeda communications reportedly have referred to inflicting a "Hiroshima" on the United States.[8] Al Qaeda's spokesman, Sulaiman Abu Ghaith, has argued that the group "has the right to kill 4 million Americans – 2 million of them children," in retaliation for the deaths the group believes the United States and Israel have inflicted on Muslims.[9] Bin Laden sought and received a religious ruling (*fatwa*) from an extreme Saudi cleric in May 2003 authorizing the use of weapons of mass destruction to kill American civilians – indeed, arguing that such use was morally obligatory if it was judged a military necessity. Then-Attorney General John Ashcroft quoted from the ruling in June 2003 before the House Judiciary Committee: "If a bomb that killed 10 million of them and burned as much of their land as they have burned Muslims land were dropped on them, it would be permissible."[10]

---

[6] [6] Rahimullah Yusufzai, "Interview with Bin Laden: World's Most Wanted Terrorist" (ABC News, 1999; available at http://www.islamistwatch.org/blogger/localstories/05-06-03/ABCInterview.html as of 5 January 2007).

[7] For useful accounts of al Qaeda's nuclear efforts, see, for example, David Albright, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents," *Nautilus Institute Special Forum* 47 (2002; available at http://www.nautilus.org/archives/fora/Special-Policy-Forum/47_Albright.html as of 2 January 2007); David Albright, Kathryn Buehler, and Holly Higgins, "Bin Laden and the Bomb," *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.isis-online.org/publications/terrorism/binladenandbomb.pdf as of 2 January 2007), pp. 23-24; Sara Daly, John Parachini, and William Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism* (Santa Monica, Cal.: RAND, 2005; available at http://www.rand.org/pubs/documented_briefings/2005/RAND_DB458.sum.pdf as of 5 January 2007). For a quick summary of open reporting on al Qaeda's efforts, see Weapons of Mass Destruction Terrorism Research Program, "Chart: Al Qa'ida's WMD Activities" (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 13 May 2005; available at http://cns.miis.edu/pubs/other/sjm_cht.htm as of 23 May 2006). For a useful discussion of the early days of al Qaeda's efforts, see text and sources in Gavin Cameron, "Multitrack Microproliferation: Lessons from Aum Shinrikyo and Al Qaeda," *Studies in Conflict and Terrorism* 22, no. 4 (October-December 1999).

[8] See James Risen and Steven Engelberg, "Signs of Change in Terror Goals Went Unheeded," *New York Times*, 14 October 2001. For an interesting discussion of the frequency with which top al Qaeda operatives express their desire for nuclear weapons, see Steve Coll, "What Bin Laden Sees in Hiroshima," *Washington Post*, 6 February 2005.

[9] Sulaiman Abu Ghaith, in a series of articles published on an al Qaeda website under the title *In the Shadow of the Lances,* in mid-2002. The series explained al Qaeda's justification for mass killing in general and the September 11 attacks in particular. I am relying here on the translation of selected passages provided in "'Why We Fight America': Al-Qa'ida Spokesman Explains September 11 and Declares Intentions to Kill 4 Million Americans with Weapons of Mass Destruction," *MEMRI (Middle East Media Research Institute) Special Dispatch*, no. 388 (2002; available at http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP38802 as of 4 April 2006). Abu Ghaith mentioned specifically that al Qaeda had a right to use weapons of mass destruction to kill this huge number of people.

[10] The testimony mentioning the ruling by Saudi cleric Nasser bin Hamed al-Fahd is in Committee on the Judiciary, *United States Department of Justice*, U.S. House of Representatives, 108th Congress, 1st Session, 5

Al Qaeda's followers believe, in effect, that they brought down the Soviet Union – that the mujahedeen's success in forcing the Soviet Union from Afghanistan was a key factor leading to the Soviet collapse. And they appear to believe that the United States, too, is a "paper tiger" which can be driven to collapse – that the 9/11 attacks inflicted grievous damage on U.S. economic power (Osama bin Laden once estimated the total cost at $1 trillion) and that still larger blows are needed to bring the United States down. As bin Laden put it in a message to his followers in December 2001, "America is in retreat by the grace of God Almighty and economic attrition is continuing up to today. But it needs further blows. The young men need to seek out the nodes of the American economy and strike the enemy's nodes."[11] The notion that major blows could cause the collapse of the United States is, in essence, al Qaeda's idea of how it will achieve victory. A nuclear blast incinerating a U.S. city would be exactly the kind of blow they want.

While most terrorist groups would not be able to make a nuclear bomb even if they had the material, it is, unfortunately, very plausible that a well-organized and well-financed group such as al Qaeda might be able to make at least a crude nuclear explosive if they could get the needed material and had time and resources to devote to the task. (This fundamental point is discussed in more detail below.) The commission appointed by President Bush to investigate U.S. intelligence capabilities and past conclusions regarding weapons of mass destruction revealed in March 2005 that in October 2001 the U.S. intelligence community assessed that al Qaeda was capable of fabricating at least a "crude" nuclear device if it could obtain the requisite nuclear material – separated plutonium or HEU. The commission also reported that the CIA's Weapons Intelligence, Nonproliferation, and Arms Control Center and its Counterterrorist Center judged in November 2001 that al-Qaeda "probably had access to nuclear expertise and facilities and that there was a real possibility of the group developing a crude nuclear device." And the commission emphasized that the documents seized from al Qaeda safe houses in Afghanistan after the overthrow of the Taliban "brought to light detailed and revealing information about the direction and progress of al-Qa'ida's radiological and nuclear ambitions," which had not been available when those earlier judgments were made.[12]

Of course, al Qaeda today is not the same group that existed before the 9/11 attacks. The previous centrally controlled, organized structure of al Qaeda has been substantially disrupted

---

June 2003 (available at http://judiciary.house.gov/media/pdfs/printers/108th/87536.PDF as of 4 April 2006). Additional details on this episode were provided by Michael Scheuer, the former head of the Central Intelligence Agency's bin Laden unit, in Steve Kroft, "Anonymous Revealed: Michael Scheuer, Former CIA Osama Bin Laden Unit Leader, Discusses Early Intelligence and Opportunities to Kill Osama Bin Laden," "60 Minutes," *CBS News*, 14 November 2004. More on the extremist Islamic scholarship regarding the killing of civilians in war (particularly "Christians" and "Jews") is discussed in Jonathan D. Halevi, "Al-Qaeda's Intellectual Legacy: New Radical Islamic Thinking Justifying the Genocide of Infidels," *Jerusalem Viewpoints*, no. 508 (1 December 2003; available at http://www.jcpa.org/jl/vp508.htm as of 4 December 2006).

[11] This argument is outlined, and bin Laden quoted, in Bruce Hoffman, *Al Qaeda, Trends in Terrorism and Future Potentialities: An Assessment*, P-8078 (Santa Monica, Cal.: RAND, 2003; available at http://www.rand.org/pubs/papers/P8078/P8078.pdf as of 4 April 2006).

[12] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President* (Washington, D.C.: WMD Commission, 2005; available at http://www.wmd.gov/report/ as of 2 January 2007), pp. 267, 271, 292.

by the worldwide campaign against the organization since the 9/11 attacks, including the destruction of al Qaeda's Afghanistan sanctuary.[13] But top officials of the U.S. government and of other governments have continued to warn that al Qaeda retains both the intention and the capability to inflict catastrophic attacks, particularly on the United States, and continues to seek weapons of mass destruction. In summarizing the global threat to U.S. interests in February 2005, the leaders of the U.S. intelligence community were unanimous in warning of the continuing desire for weapons of mass destruction on the part of al Qaeda and the global jihadist network it has spawned. CIA Director Porter Goss warned that "it may be only a matter of time before al Qaeda or another group attempts to use chemical, biological, radiological, or nuclear weapons." FBI Director Robert Mueller warned that the intelligence community is "extremely concerned with a growing body of sensitive reporting that continues to show al Qaeda's clear intention to obtain and to ultimately use some form of chemical, biological, radiological, or nuclear material in its attacks against the United States."[14] As Goss and Mueller emphasized, the threat is not only from whatever remains of the old, centralized al Qaeda, but from the global movement that has spun off from it. Some elements of this amorphous movement have aims for mass violence on a similar scale and may have some potential to pull together the required capabilities – which, as discussed below, would not necessarily require advanced scientific knowledge, large numbers of people, or significant fixed facilities.

The documents, training manuals, and other evidence recovered by coalition forces and by Western media in Afghanistan after the overthrow of the Taliban, along with other information that has appeared in the public domain (including descriptions of interviews with detainees and information put out by al Qaeda-linked organizations), present a mixed picture. On the one hand, it is clear that the overwhelming focus of the organization and the training it provided was on conventional weapons and explosives. On the other hand, the evidence makes clear that al Qaeda had a strong interest in getting all types of unconventional weapons

---

[13] For useful discussions of al Qaeda as it was before the 9/11 attacks, see, for example: National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 1st ed. (New York: Norton, 2004; available at http://www.gpoaccess.gov/911/index.html as of 30 December 2006); Anonymous, *Through Our Enemies' Eyes: Osama Bin Laden, Radical Islam, and the Future of America* (Washington, D.C.: Brassey's, 2002); Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Berkley Books, 2003); Peter L. Bergen, *Holy War, Inc.: Inside the Secret World of Osama Bin Laden*, updated edition ed. (New York: Touchstone, 2002). The *9/11 Commission Report* provides perhaps the best quick summary of the growth and development of al Qaeda, having access both to the other works cited and to the results of interrogations of key al Qaeda personnel. Anonymous, the author of *Through Our Enemies' Eyes,* has since been revealed as Michael Scheuer, a 20-year CIA veteran who was head of the agency's bin Laden unit. For a useful overview of the changed threat posed by today's al Qaeda and related groups, see, for example, Bruce Hoffman, *Does Our Counter-Terrorism Strategy Match the Threat?* CT-250-1 (Santa Monica, Calif.: RAND, 2005; available at http://www.rand.org/pubs/testimonies/2005/RAND_CT250-1.pdf as of 28 December 2006).

[14] Mueller's testimony is in [14] Mueller's testimony is in Select Committee on Intelligence, *Current and Projected National Security Threats to the United States*, U.S. Senate, 109th Congress, 16 February 2005 (available at http://www.fas.org/irp/congress/2005_hr/shrg109-61.pdf as of 4 January 2007).

– chemical, biological, radiological, and nuclear.[15] Within the category of unconventional weapons, the group and its allies appear to have devoted more effort to chemical, biological, and radiological weapons than to actual nuclear bombs – as suggested by the videotapes showing testing of poison gas on animals and the several poison-related plots that have been revealed in recent years. Nevertheless, the detailed drawings, training manuals, and other documents and physical evidence recovered by coalition forces and by Western media from caves and safe houses in post-Taliban Afghanistan confirm that highly placed al Qaeda operatives, including alleged chemical and biological commander Abu Khabbab, had been very focused on obtaining a nuclear weapons capability. Many of the discussions of nuclear weapons in the seized documents are quite unsophisticated and contain substantial errors; but some are of higher quality, including one fact about initiating a nuclear chain reaction that remains classified and could not simply have been downloaded from the internet.[16]

Al Qaeda's interest is of long standing, stretching back over a decade. Michael Scheuer, from 1996 to 1999 the head of the CIA team focused solely on Osama bin Laden, wrote in 2004 to the House and Senate Intelligence Committees that in mid- to late-1996, "CIA's Bin Laden unit acquired detailed information about the careful, professional manner in which al-Qaeda was seeking to acquire nuclear weapons." In his letter, he continued, "there could be no doubt after this date that al-Qaeda was in deadly earnest in seeking nuclear weapons."[17] The U.S. federal indictment of bin Laden for his involvement in the bombings of U.S. Embassies in Kenya and Tanzania charges that "at various times from at least as early as 1992, Usama bin Laden and Mamdouh Mahmud Salim, and others known and unknown, made efforts to obtain the components of nuclear weapons."[18] The best documented of these incidents was an attempt in 1993 to purchase HEU for a nuclear bomb in the Sudan, which has been described in some detail in court testimony of Jamal Ahmad al-Fadl, the al Qaeda operative charged with several key steps in the transaction.[19] While al-Fadl reports that al Qaeda believed the material to be HEU when it was seeking to make the purchase, it appears that the suppliers were running a scam and the material was not usable in nuclear weapons. Similarly, it appears that al Qaeda has been scammed on several other occasions in attempts to acquire what it thought was weapons-usable nuclear material.[20] Senior bin Laden lieutenant

---

[15] See, for example, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President*, pp. pp. 267-278. For a quick summary of open sources, see Weapons of Mass Destruction Terrorism Research Program, "Chart: Al Qa'ida's WMD Activities".

[16] Probably the best available unclassified summary is Albright, "Al Qaeda's Nuclear Program."

[17] Excerpts of the letter are reprinted in [17] Excerpts of the letter are reprinted in Anonymous [Michael Scheuer], "How Not to Catch a Terrorist," *Atlantic Monthly* 294, no. 5 (2004; available at http://www.theatlantic.com/doc/200412/anonymous as of 5 January 2007), p. 50.

[18] See "Text: US Grand Jury Indictment against Usama Bin Laden" (New York: United States District Court, Southern District of New York, 6 November 1998; available at http://www.fas.org/irp/news/1998/11/98110602_nlt.html as of 4 April 2006).

[19] For the full text and a useful discussion of al-Fadl's testimony, as well as a summary of other incidents related to bin Laden and nuclear weapons through mid-2001, see Kimberly McCloud and Matthew Osborne, "WMD Terrorism and Usama Bin Laden" (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 20 November 2001; available at http://cns.miis.edu/pubs/reports/binladen.htm as of 5 April 2006).

[20] See, for example, Daly, Parachini, and Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor.*

Mamdouh Mahmud Salim, arrested in Germany in 1998 and still in prison, has been charged with being the mastermind behind this attempted purchase and possibly others: as with bin Laden, the indictment of Salim charges that he was involved in an attempt to purchase uranium "for the purpose of developing nuclear weapons."[21]

In addition to this 1993 attempt, there have been repeated reports, of varying levels of credibility, regarding al Qaeda attempts to purchase nuclear materials or nuclear weapons in the former Soviet Union.[22] Scheuer in particular has emphasized that the group has been seeking to purchase stolen nuclear weapons, has "a very professional acquisition system," and "clearly has a presence in the former Soviet Union."[23]

Al Qaeda and its allies have also actively attempted to recruit individuals with nuclear weapons expertise. For example, Osama bin Laden and his deputy Ayman al-Zawahiri met at length with two senior Pakistani nuclear weapons experts, Sultan Bashiruddin Mahmood and Chaudari Abdul Majeed – both Taliban sympathizers with extreme Islamic views – and pressed them for information on making nuclear weapons. While Mahmood and Majeed deny having supplied any useful information, Pakistani intelligence officials told the *Washington Post* that the two had provided detailed technical information, in violation of Pakistan's secrecy laws, in response to bin Laden's questions.[24] Similarly, in 2000, an official of Russia's National Security Council announced that the Taliban regime had attempted to recruit a nuclear expert from a Russian facility.[25] In 1998, a scientist at one of Russia's premier nuclear weapons laboratories was arrested for spying for both the Taliban and Iraq (in this case on advanced conventional weapons designs, not nuclear weapons – though the security services announced that this was by no means the first such espionage case at that laboratory).[26]

In November 2001, Osama bin Laden boasted to a Pakistani journalist that al Qaeda already had chemical or nuclear weapons.[27] The same journalist has also reported that bin Laden's deputy, Ayman al-Zawahiri, had claimed that the group had succeeded in buying

---

[21] See discussion in Cameron, "Multitrack Microproliferation."

[22] See discussion in Cameron, "Multitrack Microproliferation"; McCloud and Osborne, "WMD Terrorism and Usama Bin Laden".

[23] See, for example, Eric Rosenberg, "Bin Laden after Nukes from Russia, CIA Expert Says," *Omaha World-Herald*, 21 November 2004.

[24] Kamran Khan and Molly Moore, "2 Nuclear Experts Briefed Bin Laden, Pakistanis Say," *Washington Post*, 12 December 2001; Kamran Khan, "Pakistan Releases Nuclear Scientists for Ramadan's End," *The Washington Post*, 16 December 2001; Peter Baker, "Pakistani Scientist Who Met Bin Laden Failed Polygraphs, Renewing Suspicions," *Washington Post*, 3 March 2002. The most thorough available account of the incident and related issues is David Albright and Holly Higgins, "A Bomb for the Ummah," *Bulletin of the Atomic Scientists* 59, no. 2 (March/April 2003; available at http://www.thebulletin.org/issues/2003/ma03/ma03albright.html as of 2 January 2007), pp. 49-55. Ummah is a term for the worldwide Islamic community.

[25] "Taliban Tries to Access Nuclear Technologies - Russian Security Council Official," *Interfax*, 7 October 2000.

[26] "Nuclear Center Worker Caught Selling Secrets," trans. BBC Summary of World Broadcasts, *Russian NTV*, 18 December 1998.

[27] Hamid Mir, "Osama Claims He Has Nukes: If US Uses N-Arms It Will Get Same Response," *Dawn*, 10 November 2001 (available at http://www.dawn.com/2001/11/10/top1.htm as of 5 January 2007). Al Qaeda members have also talked about unleashing a "Hiroshima" on the United States. See Albright, Buehler, and Higgins, "Bin Laden and the Bomb."

portable nuclear weapons from disaffected ex-Soviet nuclear scientists.[28] There is no evidence that either claim is true, but, if their remarks are accurately reported, they demonstrate that al Qaeda at its highest levels remains actively interested in obtaining a nuclear capability and has identified the insecure nuclear weapons, material, and expertise in the former Soviet Union as a potential source to satisfy those ambitions.

Fragmentary evidence suggests that al Qaeda's nuclear effort continued after the destruction of its Afghan sanctuary. The *fatwa* on nuclear use, coming in 2003, makes clear that the group's interest in nuclear weapons is by no means a thing of the past. According to press reports, al Qaeda operative Sharif al-Masri, captured in the Afghan-Pakistani border area in mid-2004, told interrogators that al Qaeda was looking to acquire nuclear materials in Europe and move them to Mexico and from there across the porous border into the United States.[29] Two militants arrested in Germany in January 2005 – one of whom was an Iraqi who had trained in al Qaeda's Afghanistan camps and was associated with alleged 9/11 planner Ramzi Bin al-Shibh – had tried to purchase uranium and had been recorded by authorities discussing specific locations to obtain uranium.[30] As then-CIA Director George Tenet summarized the situation in early 2004: "this enemy remains intent on obtaining, and using, catastrophic weapons...Al Qa'ida continues to pursue its strategic goal of obtaining a nuclear capability."[31] There can be little doubt that if al Qaeda had the opportunity to get stolen nuclear weapons or materials, they would jump at the chance.

At the same time, the limited evidence publicly available continues to suggest a broad gap between the capabilities that well-organized and capable terrorist groups *could* put together and the capabilities they *have* demonstrated to date. While a few of the documents recovered in Afghanistan do include some disturbing sophistication on nuclear subjects, many are extremely naïve. There is no hard evidence that al Qaeda has in fact pulled together the level of expertise on nuclear weapons design and manufacture that a few reasonably competent technical people who invested some months in researching the topic would in principle be able to put together from unclassified references. Similarly, despite reports that the group repeatedly encountered scam artists claiming they had weapons-usable nuclear material when they did not, there are no open source reports that al Qaeda ever acquired one of the commercially available systems for identifying isotopes, despite the relatively low cost and ready availability of such systems.

---

[28] Andrew Denton, "Enough Rope (Interview with Hamid Mir)," *Australian Broadcasting Corporation*, 22 March 2004 (available at http://www.abc.net.au/tv/enoughrope/transcripts/s1071804.htm as of 5 January 2007).
[29] Adam Zagorin, "Bordering on Nukes?" *Time* (22 November 2004), p. 19. A different report involvingrelated to movement of nuclear or radiological materials from Mexico, involving claims that several individuals had entered the United States from Mexico with the intent of carrying out a dirty bomb attack, possibly in Boston, has since been discredited.
[30] Faye Bowers, "Eavesdropping on Terror Talk in Germany," *Christian Science Monitor*, 28 January 2005; Craig Whitlock, "Germany Arrests 2 Al Qaeda Suspects; Men Accused of Planning Attacks in Iraq," *Washington Post*, 24 January 2005.
[31] Select Committee on Intelligence, *Current and Projected National Security Threats to the United States*, U.S. Senate, 108th Congress, 2nd Session, 24 February 2004 (available at http://intelligence.senate.gov/0402hrg/040224/witness.htm as of 28 February 2006).

The same lack of sophistication is reflected in some other reported incidents of al Qaeda pursuit of nuclear or radiological materials. The summaries that have been released of the interrogations of José Padilla, for example, indicate that he and his accomplice presented to top al Qaeda operative Abu Zubaydah the absurd idea that the two of them could make a nuclear bomb using instructions downloaded from the Internet.[32] Zubaydah, according to this account, expressed skepticism and suggested that a dirty bomb would be easier, but warned that this was not as easy as Padilla seemed to think either. Strikingly, "senior al Qaeda detainee #1" (apparently Zubaydah himself, since his statements describe Zubaydah's thinking) reports that Zubaydah, in discussing a dirty bomb, spoke of "explosives wrapped in uranium," again suggesting a rather low level of nuclear expertise, since uranium, which is not very radioactive, would be among the least deadly materials to use in a radiological dirty bomb. Nonetheless, Zubaydah gave Padilla and his accomplice money to travel to meet Khalid Sheikh Mohammed, another very senior al Qaeda operative, in order for Mohammed to evaluate the plan. Mohammed also thought the plan was impractical and suggested that they focus on simpler attacks (such as bombing apartment buildings by turning on the gas in an apartment and detonating it with a bomb on a timer). Thus, both Zubaydah and Mohammed were immediately skeptical of the feasibility of nuclear and radiological attacks, and Zubaydah, at least, apparently knew little about nuclear matters. It may be, however, that Zubaydah and Mohammed's skepticism was based on a low (and possibly accurate) assessment of the personal technological capabilities of Padilla and his accomplice, rather than on a view that nuclear and radiological attacks were impractical in general.

Similarly, in the case of the two al Qaeda operatives arrested in Germany in 2004 and charged with seeking uranium, the sparse information that is publicly available suggests they wanted the uranium for dispersal in a dirty bomb, rather than for use in a nuclear weapon – and the choice of uranium for that purpose again suggests a very rudimentary level of nuclear knowledge.[33] In short, more than a decade after al Qaeda's pursuit of the bomb began, there is as yet no strong, publicly available evidence that the group or its followers have put together the capabilities that would be necessary to make a nuclear bomb. But unfortunately, we simply cannot know what capabilities al Qaeda and its followers may have managed to keep hidden – or may acquire in the future.

Aum Shinrikyo

Aum Shinrikyo, the Japanese doomsday cult (now renamed Aleph) carried out a comprehensive program of development for chemical, biological, and nuclear weapons prior to its famous 1995 nerve gas attack in the Tokyo subway.[34] Aum's leader, Shoko Asahara,

---

[32] The following discussion is drawn from the extensive summary of the interrogations of Padilla and others that was released by the U.S. Department of Defense. See U.S. Department of Defense, *Summary of José Padilla's Activities with Al Qaeda* (Washington, D.C.: DOD, 2004; available at http://news.findlaw.com/nytimes/docs/padilla/pad52804dodsum5.html as of 2 January 2007).

[33] Bowers, "Eavesdropping on Terror Talk in Germany"; Whitlock, "Germany Arrests 2 Al Qaeda Suspects; Men Accused of Planning Attacks in Iraq."

[34] This account of Aum Shinrikyo's nuclear activities is drawn in substantial part from Daly, Parachini, and Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor*. Both those sources provide useful summaries of Aum Shinrikyo's nuclear efforts. Some of the most comprehensive investigations of Aum Shinrikyo's weapons

was obsessed with weapons of mass destruction, particularly nuclear weapons. The cult had tens of thousands of members at its peak; assets in the range of hundreds of millions of dollars, millions of which it spent on its chemical, biological, and nuclear weapons programs; hundreds of members with advanced technical training, in some cases from Japan's leading universities; and a substantial number of facilities where it could pursue its work in secret (prior to the Tokyo subway attack, Japanese authorities gave the group remarkably free rein, in part because of its status as a religious organization). The cult targeted Russia as a potential source of nuclear weapons, materials, and technology; reportedly succeeded in recruiting tens of thousands of members there; reportedly recruited staff members at the Kurchatov Institute[35] (one of Russia's leading nuclear research centers and a site where hundreds of kilograms of HEU was poorly secured and accounted for at the time); established extended relationships with a variety of senior Russian officials, including the chairman of Russia's Security Council; and sent senior cult officials on numerous weapons-shopping trips to Russia.

Nonetheless, Aum Shinrikyo failed to acquire nuclear weapons or the materials to make them – and apparently concluded that nuclear weapons would be sufficiently difficult and time-consuming to acquire that it should place its principal emphasis on chemical and biological weapons, in the belief that these would be easier to produce quickly, on a schedule consistent with Asahara's predictions of when doomsday would occur. While the chemical and biological programs proceeded on a remarkable scale – with more than a dozen different chemical and biological attacks, production of a wide range of agents, and construction of a facility capable of producing hundreds of kilograms of sarin nerve gas per year – the efforts were riddled with mistakes. Had Aum made fewer mistakes in producing and dispersing the sarin used in the Tokyo subway attack, the number of fatalities would have been far higher. As far as can be determined, Aum's biological attacks never killed anyone. Indeed, Aum reportedly was dispersing a non-virulent strain of anthrax used in vaccines, unaware that the anthrax it had acquired was not deadly.[36] These extensive problems in the efforts of such a

---

of mass destruction efforts available in English include Both those sources provide useful summaries of Aum Shinrikyo's nuclear efforts. Some of the most comprehensive investigations of Aum Shinrikyo's weapons of mass destruction efforts available in English include David E. Kaplan and Andrew Marshall, *The Cult at the End of the World: The Terrifying Story of the Aum Doomsday Cult, from the Subways of Tokyo to the Nuclear Arsenals of Russia*, 1st American ed. (New York: Crown Publishers, 1996). For a useful chronology of Aum's efforts related to weapons of mass destruction, with sources, see Tim Ballard et al., *Chronology of Aum Shinrikyo's Cbw Activities* (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2001; available at http://www.cns.miis.edu/pubs/reports/aum_chrn.htm as of 2 January 2007). For a useful chronology of Aum's efforts related to weapons of mass destruction, with sources, see Ballard et al., *Chronology of Aum Shinrikyo's Cbw Activities*.

[35] See, for example, discussion in U.S. Congress, Senate, Committee on Government Affairs, Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo: Staff Statement* (Washington, D.C.: U.S. Government Printing Office, 1995; available at http://www.fas.org/irp/congress/1995_rpt/aum/index.html as of 5 January 2007). The staff investigators confirmed by visiting the Kurchatov Institute and speaking with staff that at least one staff member at Kurchatov was still an Aum member months after the Tokyo nerve gas attack.

[36] For an account of Aum's chemical and biological efforts, see, for example, David E. Kaplan, "Aum Shinrikyo," in *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, ed. Jonathan B. Tucker, Bcsia Studies in International Security (Cambridge, Mass.: MIT Press, 2000). For a discussion of the

large, well-financed, and technically trained terrorist group contributed to the pre-9/11 view that terrorists crazy enough to want to cause mass death would be crazy enough to interfere with their ability to put together weapons of mass destruction.

Similarly, much of Aum's nuclear program seems to have been poorly focused. It was pursuing efforts such as purchasing a sheep farm with uranium deposits in Australia and stealing confidential documents on laser isotope enrichment, with the idea of producing HEU by mining uranium, purifying it, and using laser enrichment to separate the U-235.[37] This is perhaps the most technically demanding and difficult route to acquiring fissile material yet devised. Yet there is no public evidence that Aum pursued the apparently simpler approach of trying to steal any of the tons of separated plutonium or hundreds of kilograms of HEU that were present in Japan; during the peak of the cult's operations, Japan did not have regulatory requirements that nuclear facilities where such materials were located have armed guards on-site.

Aum did pursue the straightforward approach of seeking to acquire nuclear technology and material from the former Soviet Union. The cult put one of its leading technical experts in charge of its Russia operations. It sent a leading cult official, Kiyohide Hayakawa, on more than 20 trips to Russia, apparently in significant part weapons-buying expeditions (Hayakawa's extensive notebooks include the arresting notation "how much is a nuclear warhead?" followed by several possible prices).[38] The group even requested a meeting with then-Minister of Atomic Energy Victor Mikhailov in an attempt to purchase a nuclear weapon. While Mikhailov refused to meet with Aum, then-Russian Vice President Alexander Rutskoi and other senior officials met with an Aum delegation headed by the cult's leader, Shoko Asahara, in early 1992, and some reports assert that Aum paid between $500,000 and $1 million to Oleg Lobov, then Secretary of the Russian Security Council, between 1991 and 1995 – a charge Lobov denies. Lobov and Aum co-founded a Russian-Japanese university in Moscow, with offices that Lobov had arranged across from the Bolshoi Ballet – a sign of the extensive influence Aum enjoyed.[39]

After the 1995 sarin gas attacks in the Tokyo subway the Japanese government moved aggressively against the group's weapons of mass destruction programs and arrested most of its top leadership. An effort to ban the group entirely failed, however, though the group was banned in Russia. Nevertheless, this was not the end for Aum, or, it appears, for its interest in nuclear topics. Years later, Tokyo police were reporting that a software company founded by the cult had gained access to information on nuclear projects in several countries;[40] some

---

cult's use of a vaccine strain of anthrax, see Paul Keim et al., "Molecular Investigation of the Aum Shinrikyo Anthrax Release in Kameido, Japan," *Journal of Clinical Microbiology* 39, no. 12 (December 2001; available at http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=11724885 as of 2 June 2005).

[37] See, for example, discussion in Daly, Parachini, and Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor*.

[38] See Daly, Parachini, and Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor*.

[39] See Kyle B. Olson, "Aum Shinrikyo: Once and Future Threat?" *Emerging Infectious Diseases* 5, no. 4 (July-August 1999; available at http://www.cdc.gov/ncidod/EID/vol5no4/pdf/olson.pdf as of 2 June 2005).

[40] See, for example, "Aum Cult May Possess Plans on Overseas Nuclear Plants."

reports suggest the information included data on nuclear material transport routes.[41] While many of the group's key leaders remain in prison, the group, now known as Aleph, still has thousands of members and continues to recruit more. As recently as late 2004, the Japanese National Police Agency, in its annual report, warned of the "danger" that the cult would return to "organized illegal activities," pointing out that the cult continues to emphasize the centrality of the doctrines of founder Shoko Asahara.[42] In Russia as well, there have been concerns over continued activity of the cult, which is estimated to have some 300 active members and several facilities there, despite its status as a banned organization.[43]

In short, like the al Qaeda case, the Aum Shinrikyo case demonstrates that even large and well-financed terrorist groups with ample technical resources can have substantial difficulty following the nuclear path. In particular, it appears that despite being willing to spend millions of dollars in Russia to acquire nuclear weapons or the means to make them, the group failed to do so.

Chechen Terrorists

There is a substantial record of interest in and statements about chemical, biological, radiological, and nuclear weapons by the more extreme Chechen terrorist factions. It is important to be careful about the evidence, however, as in the ongoing conflict, Russian officials have been quick to charge the Chechens with virtually any horrific act or intention imaginable. Moreover, Chechen nationalists should not all be tarred with the same brush. By no means all Chechen nationalists support terrorist tactics, and by no means all Chechen terrorists would be interested in the scale of violence involved in a nuclear attack. Genuine Chechen nationalists, fighting for an independent Chechnya, might be reluctant to actually use a nuclear bomb against Russia, fearing that the likely response might well effectively obliterate any chance for a functional future Chechen state. (*Threatening* such use in order to blackmail Russia into withdrawing its forces, however, might be of more interest to genuine Chechen nationalists.) The best documented incident involving Chechen fighters and radiological material – the placement of cesium-137 in a popular Moscow park in 1995 – is an example of this kind of restraint: the Chechen fighters placed the material in the park and then informed the Russian media where it was, as a warning, without attempting to use the material for an actual attack.

But a range of indicators suggests that some Chechen factions may be interested in violence on a nuclear scale. The attack by 32 heavily armed and suicidal terrorists on an elementary school in Beslan in September 2004, which ended in the massacre of over 300 people, most of them children, demonstrates clearly that some Chechen factions are willing to kill innocent civilians on a large scale and are capable of organizing large and well-planned operations to do so. Some of the most prominent Chechen factions have increasingly allied themselves with an extreme Islamic agenda that is more global than local, and there have long

---

[41] "Cult Siphoned Nuclear Data," *Asahi News Service*, 29 March 2000.
[42] "Japanese Police Issue Annual Report Stressing Threat of Terrorism, Cults," *Kyodo News Service*, 7 December 2004. See also Olson, "Aum Shinrikyo: Once and Future Threat?"
[43] See, for example, "Security Agency Inspects 39 Aum-Linked Facilities in 2004," *Kyodo News Service*, 22 April 2005.

been strong ties between some Chechen factions and al Qaeda. Chechen fighters have trained in al Qaeda camps in Afghanistan, foreign al Qaeda fighters have fought in Chechnya, and Chechen fighters have fought for the Taliban and al Qaeda in Afghanistan.[44] The most extreme Islamist factions might be tempted to use a weapon of mass destruction against Russia – or some groups might provide such weapons to al Qaeda for use elsewhere, making the ongoing conflict in Chechnya potentially a global danger.[45]

Some statements by Chechen terrorists and documents seized from them have suggested an interest in large-scale nuclear terrorism – either by sabotage of a major nuclear facility or use of a nuclear bomb – and Chechen terrorists have repeatedly indicated an interest in the use of radiological weapons.[46] As one recent example – suggesting the tension within the Chechen camp between those who support and oppose nuclear terrorism – Akhmed Zakayev, an envoy for then-Chechen leader Aslan Maskhadov, warned that additional terrorist attacks in Russia were likely and that: "We cannot exclude that some group takes over some nuclear facility. The results may be catastrophic, not only for Russian society and for Chechen society, but for the whole of Europe."[47] Though not specifically mentioning nuclear weapons, the late Chechen warlord Shamil Basayev – who took responsibility for the Beslan attack – told the *Globe and Mail* newspaper in October 2004 that he would use any means to force Russia to give Chechnya independence, including the use of chemical and biological weapons against civilians.[48] During 2004-2005, some Chechen elements increasingly adopted a radical jihadist agenda; in July 2004, shortly before the Beslan attacks, even Maskhadov, a relative moderate and long-time opponent of the tactics used by Basayev and others, gave an interview in which he said that attacks on Russian cities would be legitimate and praised Basayev as continuing "to battle the occupiers successfully."[49] Maskhadov was killed by Russian security forces in early 2005 and replaced with a more

---

[44] For a short and useful summary, see Andrew Higgins, Guy Chazan, and Gregory L. White, "Battlefield Conversion: How Russia's Chechen Quagmire Became Front for Radical Islam," *Wall Street Journal*, 16 September 2004. The *9/11 Commission Report* also discusses involvement of international Islamic terrorists in Chechnya. See, for example, National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, pp. 58, 125, 149. A document of uncertain provenance acquired by the Defense Intelligence Agency in 1998, which purports to be a history of al Qaeda, goes so far as to say that the late Chechen rebel leader Khattab, leader of the foreign *jihadis* in Chechnya, was sent to Chechnya specifically by Osama bin Laden. The document was released in redacted form as a result of a Freedom of Information Act suit by Judicial Watch. See *Swift Knight -- Usam Ben Laden's Current and Historical Activities* (1998; available at http://www.judicialwatch.org/cases/102/dia.pdf as of 8 December 2006).

[45] For a useful discussion, see Christina Chuen, "Chechnya Has Become a Danger to Us All: A Conduit for Loose Nukes," *International Herald Tribune*, 26 June 2004.

[46] See the summary in Simon Saradzhyan, *Russia: Grasping Reality of Nuclear Terror* (Cambridge, Mass.: Belfer Center for Science and International Affairs, 2003; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/saradzhyan_2003_02.pdf as of 2 January 2007). Vladimir Orlov, director of the PIR Center, Russia's leading nonproliferation research group, has compiled a list of 25 incidents of Chechen threats or actions relating to nuclear or radiological weapons. Remarks to the 2004 Carnegie International Nonproliferation Conference, Washington DC, June 21-22, 2004.

[47] Gleb Bryanski, "Interview: Chechens Could Strike Nuclear Plant Next," *Reuters*, 27 October 2002.

[48] Mark MacKinnon, "Will Use Any Tactic, Chechen Warlord Warns," *Globe and Mail*, 2 November 2004.

[49] "Text: Excerpts of Reuters Interview with Chechen Rebel Leader," *Reuters*, 18 July 2004.

radical leader from the Chechen Sharia Council, who has said the Chechens will no longer ask Russia for peace.[50]

In January 2002, Russian troops found what they described as the personal archive of the late Chechen president Dzhokhar Dudayev, which contained a detailed plan to hijack a Russian nuclear submarine.[51] The commander of Russia's troops in Chechnya, Colonel-General Vladimir Moltenskoi, told reporters on February 2, 2002, that the plan provided for seven Slavic-looking fighters to seize a submarine from the Russian Navy's Pacific Fleet some time in 1995-96 and blackmail Moscow into withdrawing troops from Chechnya and recognizing the republic as an independent state.[52] Moltenskoi reported that former naval officer Islam Khasukhanov developed the plan back in 1995 and that then-chief of the Chechen General Staff Maskhadov had personally reviewed the plan and made notes on it. Khasukhanov had served on Russian submarines before leaving the Pacific Fleet in the rank of naval commander to become chief of the operational department of the Chechen separatists' general staff.[53]

In 2003, Yuri Vishenvsky, then-chairman of Russia's nuclear regulatory agency, said that "information from the power agencies indicates that there have been attempted attacks" on Russian nuclear facilities by Chechen terrorists.[54] Similarly, as noted at the beginning of this section, the Russian state newspaper has reported that the 41 heavily armed terrorists who seized a theater in Moscow in October 2002 considered seizing the Kurchatov Institute instead. While the Kurchatov Institute has enough HEU on-site for dozens of nuclear weapons, the press report, based on information from Russian security services, suggested that the plan the terrorists considered involved not stealing HEU but seizing a reactor at Kurchatov, threatening to blow it up if their demands were not met.[55]

Most disturbing are the specific incidents which suggest Chechen terrorist interest in stealing nuclear weapons or weapons-usable nuclear material. These include, most notably, the incidents sited at the outset of this section, in which terrorist teams carried out

---

[50] "Chechen Rebel Says Will Never Ask Russia for Peace," *Reuters*, 16 May 2005.

[51] "Russian TV Says Chechen Rebels Plotted to Seize Nuclear Submarine.," *Interfax*, 27 April 2002; "Nachalnik Operativnogo Shtaba Maskhadova Gotovil Plan Zakhvata Rosiiskoi Atomnoi Podlodki (Chief of Maskhadov's Operational Staff Was Preparing a Plan to Hijack Russian Atomic Submarine)," *RIA-Novosti*, 25 April 2002. The second of these articles is summarized in Saradzhyan, *Grasping Reality of Nuclear Terror.*

[52] Russian *RTR* Television reported on April 26, 2002, that the plan included removing a nuclear warhead from the submarine and bringing it back to Chechnya. See "Russian TV Says Chechen Rebels Plotted to Seize Nuclear Submarine." No other media confirmed this report, however. The Pacific Fleet presently operates no nuclear-powered ballistic missile submarines (SSBNs), but it still has some 20 nuclear powered submarines, including those of the Oscar-II class that can carry nuclear torpedoes. Under the 1991-1992 Presidential Nuclear Initiatives, however, all of these nuclear weapons should have been removed from the submarines – so if this commitment had been fulfilled, seizing a submarine would not have allowed the group to seize a nuclear weapon as well. When the plan was reportedly developed in 1995, however, this commitment to remove tactical nuclear weapons from naval ships may not yet have been fully implemented – or may not have been noticed by those planning this possible attack. Some nuclear weapons are believed to remain in a storage site for the Pacific Fleet whose security has been upgraded with U.S. assistance.

[53] "Chief of Maskhadov's Operational Staff Was Preparing a Plan."

[54] "Nuclear Security Hiked against Chechen Threat," *Moscow Times*, 21 February 2003.

[55] Bogdanov, "A Pass to Warheads Found on a Terrorist."

reconnaissance at nuclear warhead storage facilities and, reportedly, on nuclear warhead transport trains. Another disturbing incident occurred in March 2002, when Russian police in the Sverdlovsk region arrested three Chechens in possession of a range of guns and explosives. One of the men was found to have a valid pass to the high-security closed city of Lesnoy, site of one of Russia's largest nuclear weapons assembly and disassembly facilities. (This pass would have entitled him to enter the closed city, but not the weapons facility itself, though he could have used his access to the city to build relationships with employees and guards at the weapons facility.) He had the pass because his father had been an employee at the plant and the family had lived in the city.[56] In January 2003, Colonel-General Igor Valynkin, commander of the 12th Main Directorate of the Russian Ministry of Defense, the branch responsible for guarding Russia's nuclear weapons, summed up the situation by warning that "Chechen terrorists plan to seize some crucial military facility or nuclear warhead so as to threaten not just Russia, but the whole world."[57] In late 2005, Russian Interior Minister Rashid Nurgaliev, in charge of the troops that guard most key nuclear facilities in Russia, confirmed that in recent years "international terrorists have planned attacks against nuclear and power industry installations" intended to "seize nuclear materials and use them to build weapons of mass destruction for their own political ends."[58] Although Nurgaliev referred generally to "international terrorists," rather than to "Chechen terrorists," he probably had groups that were primarily Chechen in mind, as Valynkin did; Russian officials frequently assert that Chechen terrorists are being assisted by outsiders linked to al Qaeda, and lump both together. (The renowned Chechen leader Khattab was a Jordanian, who by some accounts had strong links to al Qaeda.)

Chechen groups might well be able to pull together the capabilities needed to acquire nuclear weapons or materials in Russia, though there is no solid evidence that they have done so to date. Attacks such as Beslan demonstrate Chechen terrorists' ability to pull together attacks involving dozens of fighters striking at once, without warning; armament including machine guns, rocket-propelled grenades, and large quantities of explosives; and help from current or former members of Russia's policy and security services. Many nuclear facilities would find it difficult to defend against a no-warning attack on that scale. Similarly, the problem of theft by corrupt or blackmailed insiders is potentially a serious one; insider thefts of weapons from military facilities and of equipment from nuclear facilities occur routinely in Russia,[59] and Chechen fighters have regularly made use of both corrupt insiders and tactics such as kidnapping family members of individuals they wish to blackmail. Indeed, a number of police and security officials have been arrested for their assistance in Chechen terrorist attacks.[60] Chechen terrorist groups are thought to have ties with Chechen organized crime

---

[56] See, for example, Sergei Avdeyev, "Chechens Gain Access to Nuclear Warheads," *Izvestia*, 22 March 2002; Bogdanov, "A Pass to Warheads Found on a Terrorist."

[57] Sergei Ostanin, "Chechen Terrorists out to Lay Hands on Nuclear Arms -- Military," *ITAR-TASS*, 30 January 2003.

[58] "Internal Troops to Make Russian State Facilities Less Vulnerable to Terrorists," *RIA-Novosti*, 5 October 2005.

[59] Bunn, "Anecdotes of Insecurity."

[60] For a discussion of several cases and their implications, see Simon Saradzhyan and Nabi Abdullaev, "Disrupting Escalation of Terror in Russia to Prevent Catastrophic Attacks," *Connections* (Spring 2005).

groups, which in turn are thought to have ties with Russian organized crime. These and other Chechen terrorist contacts in Russia could increase their potential to acquire nuclear weapons or materials.

In short, in the last decade, three different terrorist groups in three different contexts have actively sought nuclear weapons, including attempting to buy or steal nuclear weapons or their essential ingredients, or at least carrying out surveillance in possible preparation for such an effort. The world cannot assume that these groups will be the last. Even if al Qaeda could somehow be destroyed completely, the threat of nuclear terrorism would be reduced, not eliminated.

Iraq

States, in general, are likely to be very different from terrorist groups – having stable control over large land areas and fixed facilities and far larger resources of both money and personnel to apply to their military programs. For most states seeking nuclear weapons, the first preference would be an indigenous ability to produce their own nuclear material and their own nuclear weapons. But such capabilities are expensive and difficult to get. The historical record indicates that states do indeed consider buying a bomb or the materials to make one if (a) they believe they can avoid the expense and difficulty of putting together their own nuclear material production facilities; (b) they see an urgent need to establish a nuclear deterrent before their own nuclear material production succeeds; or (c) they face an international nonproliferation effort that is making it very difficult to successfully establish their own nuclear material production facilities. Acquiring stolen nuclear material from abroad could offer an extraordinarily valuable shortcut, cutting a proliferator's bomb program from years to months, or even less, if other necessary preparations had already been made. Making a bomb from nuclear material already in hand might be done both quickly and in facilities that might remain covert, presenting the international community with a terrifying new threat with very little warning.

Consideration of buying a nuclear weapon or the material to make one is not unusual in the historical record. Australia wanted to purchase a nuclear weapon, when it was considering the nuclear weapons option; Egypt explored the possibility of a purchase when it was pursuing a nuclear weapons program; Libya, realizing the weakness of its own indigenous science and technology base, is reported to have repeatedly attempted to purchase a nuclear weapon, including an unsuccessful approach to China; there are even reports that Indonesia sought to purchase a bomb, decades ago.[61] In short, the cases of Iraq and Iran, described below, are not unique and should be considered only as particular case studies of a broader phenomenon. The more nonproliferation efforts focused on limiting states' ability to

[61] Jim Walsh, "Bombs Unbuilt: Power, Ideas, and Institutions in International Politics" (Ph.D. dissertation, Political Science, Massachusetts Institute of Technology, 2001); Joseph Cirincione, Jon B. Wolfsthal, and Miriam Rajkumar, "Libya," in *Deadly Arsenals: Nuclear Biological, and Chemical Threats* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.carnegieendowment.org/pdf/npp/18-Libya.pdf as of 10 December 2006); Robert M. Cornejo, "When Sukarno Sought the Bomb: Indonesian Nuclear Aspirations in the Mid-1960s," *Nonproliferation Review* 7, no. 2 (Summer 2000; available at http://cns.miis.edu/pubs/npr/vol07/72/72corn.pdf as of 10 December 2006).

build their own enrichment and reprocessing facilities succeed in the future, the more likely it is that additional states will pursue the purchase alternative.

It was long a worry that Iraq might exploit such an opportunity, given its substantial nuclear weapons program prior to the 1991 Gulf War and given its apparent interest in a covert nuclear breakthrough after that war. But the available evidence suggests that despite some attempts, Iraq was not able to acquire weapons-usable material before 1991 and may not have tried seriously after 1991. Since the U.S.-led invasion that overthrew Saddam Hussein in 2003, intelligence assessments on Iraq's weapons of mass destruction program prior to the war have proven to be wildly wrong – and therefore considerable care has to be taken in assessing the available evidence concerning Iraq's efforts to acquire black market nuclear material.

There is no dispute that Iraq's former leader Saddam Hussein spent billions of dollars before the 1991 Gulf War attempting to establish an indigenous Iraqi capability to produce fissile material.[62] This effort included the creation of a far-ranging procurement network involving large numbers of agents, front companies, and the like, which succeeded in illicitly acquiring a wide range of nuclear-related technologies from countries around the world.

While the network's principal focus was on the technologies that would permit the establishment of indigenous Iraqi production of nuclear bomb material, it seems certain that pre-1991 Iraq would have snapped up weapons-usable nuclear material eagerly, had its agents been able to find a reliable source from which to buy it. Indeed, in its declarations to international inspectors after the 1991 war, Iraq eventually acknowledged that it had purchased non-weapons-usable natural uranium for its indigenous production program on more than one occasion – demonstrating its willingness to purchase nuclear material illicitly.[63] During the 1990s, Iraqi officials claimed to international inspectors that before the 1991 war, Iraq had received many offers of stolen nuclear materials for its weapons program, but had turned them all down – a claim that is difficult to credit.[64] At least one participant in Iraq's

---

[62] For overviews, see Charles Duelfer, "Volume II: Nuclear," in *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at http://www.foia.cia.gov/duelfer/Iraqs_WMD_Vol2.pdf as of 10 December 2006); Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President*; International Atomic Energy Agency, *Fourth Consolidated Report of the Director General of the International Atomic Energy Agency under Paragraph 16 of Security Council Resolution 1051 (1996)*, S/1997/779 (New York: United Nations, 1997; available at http://www.iaea.org/worldatom/Programmes/ActionTeam/reports/s_1997_779.pdf as of 10 December 2006); Gary Samore, ed., *Iraq's Weapons of Mass Destruction: A Net Assessment* (London: International Institute for Strategic Studies, 2002); David Albright, *Iraq's Programs to Make Highly Enriched Uranium and Plutonium for Nuclear Weapons Prior to the Gulf War* (Washington, D.C.: Institute for Science and International Security, 2002; available at http://www.isis-online.org/publications/iraq/iraqs_fm_history.html as of 10 December 2006); Rodney W. Jones and Mark G. McDonough, *Tracking Nuclear Proliferation: A Guide in Maps and Charts* (Washington D.C: Carnegie Endowment for International Peace, 1998; available at http://www.ceip.org/programs/npp/track98b.htm as of 10 December 2006). I have not included here the now-discredited dossiers on the subject from U.S. and British intelligence released in the debate leading up to the 2003 war.

[63] See Duelfer, "Volume II: Nuclear," p. 9.

[64] One senior Iraqi official told inspectors in 1996 that Iraq had received over 200 offers of everything from red mercury to fissile material for its nuclear weapons program over the preceding decade. See discussion in David

bomb program during the period before the 1991 war, Khidir Hamza, tells the opposite story. Hamza reports that when arms dealers from the Soviet Union and Eastern Europe with whom Iraq had an ongoing relationship made offers of plutonium or highly enriched uranium, Iraqi authorities told them they were interested and gave them cash to acquire samples. In every case of which Hamza was aware, however, the samples turned out to be radioactive trash, not plutonium or HEU.[65] As a result of these experiences, and out of fear of being caught by a Western sting operation, Hamza reports that the part of Iraq's nuclear weapons program with which he was associated began rejecting outside offers – though Hamza expressed his belief before the second Gulf War that Iraqi military intelligence continued to pursue them. Hamza acknowledged that had any of the samples proved to be genuine weapons-usable nuclear material, Iraq would have been eager to purchase as much as was available.[66]

The accuracy of many of Hamza's assertions, particularly about the importance of his own role in Iraq's pre-war nuclear weapons program, has been extensively challenged.[67] His assertions regarding attempted purchases of nuclear material nevertheless seem credible, because (a) they were detailed and described as incidents in which he had personally taken part; (b) they ran contrary to the overall point he was attempting to make, which was that the principal danger was Iraq's potential to establish indigenous production capabilities, and so cannot be explained as having been made up to support a larger argument; and (c) they fit reasonably well with known facts concerning the extensive foreign Iraqi procurement network. But they remain assertions from a single source of uncertain reliability. If they *are* correct, they are particularly notable because of the timing of the incidents described: Hamza left the Iraqi program in late 1990, so his account would imply that arms dealers from the Soviet Union and Eastern Europe were claiming to be able to provide stolen plutonium and HEU *before* the Soviet Union collapsed. (The official Iraqi statement that Iraq received multiple offers of nuclear material which it turned down before the 1991 war carries the same implication, since the Soviet Union did not collapse until the end of 1991.)

Albright and Khidhir Hamza, "Iraq's Reconstitution of Its Nuclear Weapons Program," *Arms Control Today* 28 (October 1998; available at http://www.armscontrol.org/act/1998_10/daoc98.asp as of 27 February 2006).

[65] Khidir Hamza, personal communication, September 2002. In an earlier interview with *Frontline,* Public Broadcasting System, he reports that Iraq attempted to get nuclear weapons and materials from the former Soviet Union, but was unable to do so and found the market full of both black marketers unable to deliver what they promised and sting operations by governments (a problem he also mentioned in his September 2002 discussion with me). See "Interview with Khidhir Hamza" in *Frontline: Gunning for Saddam*, ed. (Washington, D.C.: Public Broadcasting System, 2001; available at http://www.pbs.org/wgbh/pages/frontline/shows/gunning/interviews/hamza.html as of 10 December 2006). In another interview, Hamza describes Iraqi bribery in the Soviet Union to acquire advanced weapons technologies during the Iran-Iraq war, but does not mention attempts to get nuclear technologies by this route. See "Saddam's Bombmaker," "60 Minutes II," *CBS News*, 27 January 1999.

[66] Khidir Hamza, personal communication, September 2002.

[67] See, for example, quotes from an unnamed IAEA staffer and from former Hamza co-author David Albright in Michael Massing, "Now They Tell Us," *New York Review of Books* 51, no. 3 (26 February 2004; available at http://foi.missouri.edu/polinfoprop/nowtheytell.html as of 10 December 2006); Patrick Cockburn, "America Quietly Sacks Its Prize Witness against Saddam," *Independent*, 17 April 2004 (available at http://www.commondreams.org/headlines04/0417-12.htm as of 10 December 2006).

The potentially critical importance of getting enough nuclear material for one bomb, while the ability to make more was still being put in place, became clear after Iraq's invasion of Kuwait. Seeing the U.S. and coalition response to that invasion, Iraq launched a "crash" program to rapidly produce a single bomb. For that purpose it planned on using HEU from its French-supplied and Soviet-supplied research reactors, material that was under International Atomic Energy Agency (IAEA) safeguards.[68] As the availability of sufficient quantities of adequately pure and enriched HEU was a key limiting factor for this effort, Iraq surely would have been eager to receive HEU from a nuclear black market during the period of the "crash" program. Whether Iraq's extensive foreign procurement effort was given explicit orders to attempt to acquire such material at that time is not known. With the coalition attack in 1991, the crash program ran out of time.

It appears that the 1991 Gulf War and the intrusive international inspections that followed effectively put an end to the Iraqi nuclear weapons program. The Iraq Survey Group (ISG), the U.S. team set up after the U.S.-led invasion of Iraq in 2003 to examine the nature and scope of Iraqi WMD programs, concluded that "Saddam [Hussein] ended the nuclear program in 1991 following the Gulf war. ISG found no evidence to suggest concerted efforts to restart the program."[69] This conclusion is effectively identical to those of the IAEA inspection teams, but stands in stark contrast to the claims made by the Bush administration prior to the 2003 U.S.-led invasion of Iraq. Despite pre-war statements to the contrary, the ISG also found no evidence that Iraq sought uranium from abroad after 1991.[70] The commission established to review U.S. intelligence on weapons of mass destruction after the 2003 war strongly supported the ISG's conclusions.[71]

The ISG report does document that despite UN inspections and sanctions after the 1991 war, Iraq continued an extensive procurement effort focused on acquiring a wide range of military technologies prohibited under the UN sanctions regime, including technologies and materials acquired from entities in countries such as Belarus, Russia, Ukraine, Yugoslavia, and Romania (all of which held weapons-usable nuclear material that was dangerously insecure at the time), among many others.[72] Iraq succeeded, for example, in buying gyroscopes and other missile guidance instruments which were taken directly from decommissioned Russian strategic nuclear missiles and which had been tested and certified by a leading Russian institute. Desperate Russian institutes also agreed to sell a wide variety of other key missile technologies.[73] As noted earlier, an employee of Russia's premier nuclear weapons laboratory, arrested in December 1998, was accused of spying both for the Taliban

---

[68] See discussion, for example, in Samore, ed., *Iraq's Weapons of Mass Destruction.*

[69] Duelfer, "Volume II: Nuclear," p. 1.

[70] Duelfer, "Volume II: Nuclear," p. 9.

[71] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President.*

[72] Charles Duelfer, "Volume I: Regime Finance and Procurement," in *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at http://www.foia.cia.gov/duelfer/Iraqs_WMD_Vol1.pdf as of 10 December 2006).

[73] For a detailed account, see Vladimir Orlov and William C. Potter, "The Mystery of the Sunken Gyros," *Bulletin of the Atomic Scientists* 54, no. 6 (November/December 1998; available at http://cns.miis.edu/research/iraq/gyro/index.htm as of 10 December 2006), pp. 34-39.

and for Iraq – in this case on advanced conventional weapons. These efforts continued right up to beginning of the 2003 war. The ISG report, however, contains no mention of any post-1991 Iraqi effort to acquire black-market nuclear material. The only specific such case that has been reported in the public record is the assertion by the Department of Defense official who led Project Sapphire, the removal of HEU from an insecure site in Kazakhstan in the Clinton administration, that Iraq had offered $16,000 per kilogram for the HEU at that site (at some time prior to 1994, when the material was airlifted to the United States).[74] It is notable, however, that this charge is not repeated in the ISG report.

The ISG report, however, makes a persuasive argument that Saddam Hussein remained intensely interested in resuming the quest for nuclear weapons after UN sanctions were eventually lifted and that the Iraqi regime took at least modest steps to ensure that the knowledge of the participants in Iraq's nuclear weapons program was not dispersed. In the words of one Saddam directive quoted in the report: "Keep nuclear scientists together at the IAEC [Iraq Atomic Energy Commission] in order to pool their skills and have them available when needed."[75] With the HEU that was to have been used in the crash program removed from Iraq by international inspectors, acquiring stolen weapons-usable nuclear material would have been a critical way to maintain a secret nuclear capability. Indeed, from 1991 to 2003, there was a broad consensus among experts on Iraq's program that the only way it could achieve a nuclear weapons capability quickly would be by pursuing the theft option. The U.S. Central Intelligence Agency warned in 1998 (well before the shift toward more alarming assessments in the run-up to the 2003 war) that Iraq "would seize any opportunity to buy nuclear weapons materials or a complete weapon."[76] The U.S. Senate's report on pre-war intelligence on Iraq's weapons of mass destruction declares that a series of U.S. intelligence analyses from 1997 on were "consistent" in assessing that if Iraq got the needed nuclear material from abroad "it could have a crude nuclear weapon within a year," but that it would take "five to seven years" for it to make enough nuclear material for a bomb on its own, even with substantial foreign assistance.[77] Similarly, both Khidir Hamza and the IAEA inspectors in Iraq emphasized that if Iraq had acquired enough nuclear material for a bomb, the small-scale effort needed to turn it into a bomb might have been difficult for inspectors to find.[78] In

---

[74] Jeffrey Starr, quoted in Chris Flores, "Project Sapphire: A Nuclear Odyssey: Defusing a Lethal Legacy," *News & Advance*, 29 December 2002. Other accounts of Sapphire mention a concern about Iranian interest in the HEU, but not a concern about Iraq.

[75] Frontispiece quote, in Duelfer, "Volume II: Nuclear."

[76] John Deutch, then Director of Central Intelligence, prepared testimony in [76] John Deutch, then Director of Central Intelligence, prepared testimony in Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction, Part II*, U.S. Senate, 104th Congress, 2nd Session, 13, 20, and 22 March 1996.

[77] U.S. Senate, Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Assessments on Iraq* (2004; available at http://www.gpoaccess.gov/serialset/creports/iraq.html as of 11 December 2006), pp. 84-85.

[78] As the IAEA diplomatically put it, "it must be recognised that Iraq's direct acquisition of weapon-usable material would present a serious technical challenge to OMV [ongoing monitoring and verification] measures, and great reliance must continue to be placed on international controls." International Atomic Energy Agency, *Sixth Consolidated Report of the Director General of the International Atomic Energy Agency under Paragraph*

short, there was ample reason to believe before the 2003 war that, regardless of the true extent of the Iraqi nuclear program, Saddam had a strong incentive to acquire stolen nuclear material that might have made a small, covert bomb effort possible.

Nevertheless, the evidence now available suggests that Iraq did not make any strong and consistent effort to get black market nuclear bomb material after 1991, or to take any other substantial steps to reconstitute Iraq's nuclear weapons program, preferring to focus first on getting UN sanctions lifted and return to the pursuit of WMD after that had been accomplished.[79]

Iran

Because Iran retains a highly secretive government and has never been under the level of intense international inspection that Iraq faced, information about its procurement efforts is even more fragmentary than it is in the case of Iraq – but the available information suggests that Iran, too, while focusing primarily on establishing the capability to produce its own fissile material, has also sought to purchase stolen nuclear material.[80]

Like Iraq, Iran built a substantial illicit procurement network to acquire technologies related to weapons of mass destruction and ballistic missiles all over the world – including in the former Soviet Union. Like Iraq, Iran has succeeded in acquiring key missile technologies from Russian institutes and has specifically sought technologies for producing both HEU and plutonium.[81] Indeed, U.S. concerns over leakage of Russian weapons of mass destruction technologies to Iran have been central issues in U.S.-Russian relations for most of the period since the Soviet collapse. While it is now clear that the most critical technologies for Iran's indigenous efforts to produce nuclear material were coming from the black-market nuclear network led by Pakistan's Abdul Qadeer Khan, not from Russia, Iran's nuclear connections in the former Soviet Union are strong, and there are significant suggestions of ongoing efforts to acquire stolen nuclear material.

In 1996, the CIA warned that Iran was pursuing an indigenous production capability for both plutonium and HEU and that "to shorten the timeline to a weapon, Iran has launched

---

16 of UNSC Resolution 1051 (1996) (New York: United Nations, 1998; available at http://www.nci.org/i/iaea10-8-98.htm as of 11 December 2006).

[79] "Key Findings," in Charles Duelfer, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at https://www.cia.gov/cia/reports/iraq_wmd_2004/index.html as of 10 December 2006).

[80] For an overview of Iran's efforts, see Gary Samore, ed., *Iran's Strategic Weapons Programmes: A Net Assessment* (London: Taylor & Francis for the International Institute for Strategic Studies, 2005). For mid-1996 assessments of the centrifuge program specifically, see David Albright, "When Could Iran Get the Bomb?" *Bulletin of the Atomic Scientists* 62, no. 4 (July/August 2006; available at http://www.thebulletin.org/article.php?art_ofn=ja06albright as of 5 December 2006), pp. 26-33; David Albright and Corey Hinderstein, "Iran's Next Steps: Final Tests and the Construction of a Uranium Enrichment Plant" (Washington, D.C.: Institute for Science and International Security, 12 January 2006; available at http://www.isis-online.org/publications/iran/irancascade.pdf as of 6 April 2006).

[81] For a discussion of Iran's attempts to acquire sensitive nuclear technologies from Russia in particular, see, for example, Robert J. Einhorn and Gary Samore, "Ending Russian Assistance to Iran's Nuclear Bomb," *Survival* 44, no. 2 (May 2002); Jones and McDonough, *Tracking Nuclear Proliferation*, pp. 169-175.

a parallel effort to purchase fissile material, mainly from sources in the former Soviet Union."[82] The next year, the Department of Defense pointed out that the "shortest route" for Iran to get nuclear weapons would be "acquisition of a nuclear weapon from a foreign source" or to "purchase or steal fissile material."[83] In 2000, the CIA was still warning that "Tehran continues to seek fissile material"[84] and reportedly concluded that it could not rule out the possibility that Iran had already acquired a nuclear weapon capability, if it had succeeded in secretly procuring fissile material abroad.[85] In 2001, the Department of Defense again concluded that Iran is "is seeking fissile material and technology for weapons development through an elaborate system of military andd civilian organizations."[86] In 2004, the CIA warned that it "suspects" that "Tehran is interested in acquiring fissile material... from foreign suppliers" for its nuclear weapons program.[87]

During 2003-2006, after the revelation of Iran's secret centrifuge enrichment program in 2002, a series of IAEA reports documented Iran's decades-long secret effort to develop uranium enrichment and other key technologies for producing potential nuclear weapons materials.[88] Iran successfully procured a wide range of centrifuge- and laser enrichment-related technologies through the black-market network led by Pakistan's A.Q. Khan and through contacts with entities in Russia and elsewhere. Like Iraq before 1991, Iran illicitly imported large quantities of uranium without reporting these acquisitions to the IAEA. Iran repeatedly violated its safeguards obligations, both in failing to report imports and activities to the IAEA and in providing information to the IAEA that Iran now acknowledges was false. In early 2006, Iran ended a suspension of uranium enrichment activities it had agreed to with European negotiators, and by April of 2006, Iran announced that it was successfully enriching uranium in a 164-centrifuge cascade. The IAEA Board of Governors found Iran to be in violation of its safeguards agreement and reported Iran's activities to the UN Security Council. The Security Council issued a statement in April 2006 requesting that Iran again suspend enrichment and reprocessing-related activities, return to compliance with the

---

[82] Quoted in Jones and McDonough, *Tracking Nuclear Proliferation*, p. 169.

[83] U.S. Department of Defense, *Proliferation: Threat and Response* (Washington, D.C.: DOD, 1997; available at http://www.defenselink.mil/pubs/prolif97/ as of 18 December 2006).

[84] See U.S. Central Intelligence Agency, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January through 30 June 1999* (Langley, Vir.: CIA, 2000; available at https://www.cia.gov/cia/reports/721_reports/jan_jun1999.html as of 18 December 2006).

[85] See James Risen and Judith Miller, "C.I.A. Tells Clinton an Iranian a-Bomb Can't Be Ruled Out," *New York Times*, 17 January 2000 (available at http://www.library.cornell.edu/colldev/mideast/iranbmba.htm as of 18 December 2006).

[86] U.S. Department of Defense, *Proliferation: Threat and Response* (Washington, D.C.: DOD, 2001; available at http://www.defenselink.mil/pubs/ptr20010110.pdf as of 18 December 2006), pp. 34-35.

[87] See U.S. Central Intelligence Agency, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January through 30 June 2003* (Langley, Vir.: CIA, 2004; available at https://www.cia.gov/cia/reports/721_reports/jan_jun2003.htm as of 18 December 2006).

[88] The complete set of IAEA reports on implementation of safeguards in Iran, relevant Security Council statements and resolutions, and related materials, can be found at International Atomic Energy Agency, "In Focus: IAEA and Iran" (Vienna: IAEA, 2006; available at http://www.iaea.org/NewsCenter/Focus/IaeaIran/index.shtml as of 5 May 2006).

Additional Protocol strengthening safeguards, and take other steps to build confidence. Iran declined to take those steps. In July 2006, the Security Council passed resolution 1696, which legally required Iran to take those steps. Iran again refused to do so. In December 2006, after months of debate among the permanent members, the Security Council passed resolution 1737, imposing limited sanctions on Iran for its failure to comply with its obligations under resolution 1696.[89]

The IAEA reports on Iran's nuclear activity indicate that Iran's indigenous enrichment program has been underway since 1985, yet a significant degree of enrichment was first achieved in a small cascade in early 2006, more than twenty years later. Since Iran was for so long unable to produce significant quantities of weapons-usable material domestically, some in Iran might have perceived a strong incentive to acquire weapons-usable nuclear material from abroad. The IAEA's detection of HEU contamination of equipment at some facilities in Iran initially seemed to suggest either that Iran had succeeded in producing some HEU itself, or that it had received HEU from foreign sources. The detection of 36% enriched HEU, a level of enrichment used in Soviet-supplied research reactors, seemed to suggest that Iran might have gotten such material from abroad. Iran has stated that the HEU particles came from contaminated equipment Iran received from abroad (much of it originating in Pakistan, but also including some non-centrifuge equipment from Russia that may have been the origin of the 36% enrichment). In November, 2004, the IAEA reported that its "overall assessment" is that the data "tends, on balance, to support Iran's statement on the origin of much of the contamination," though other explanations continued to be investigated.[90] As of late 2006, there is no compelling evidence that these HEU particles came from black-market HEU.

There have been innumerable press reports (of varying levels of credibility) related to Iranian attempts to acquire nuclear materials or even nuclear weapons. There have also been a significant number of actual arrests of Iranian nationals apparently associated with the

---

[89] Resolutions 1696 and 1737 can be found at International Atomic Energy Agency, "IAEA and Iran".

[90] International Atomic Energy Agency, *Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran*, GOV/2004/83 (Vienna: IAEA, 2004; available at http://www.iaea.org/Publications/Documents/Board/2004/gov2004-83.pdf as of 18 December 2006), pp. 9-10. The November 2004 report states that environmental samples of domestically produced components showed predominantly LEU contamination and that it was on the imported components that LEU and HEU particles had been found. Particles at enrichment levels up to 70% uranium-235 concentration were found in samples taken from imported components in several different locations. Particles of approximately 54% HEU were found on imported components and centrifuge rotors constructed using imported components, and some 54% HEU was also detected in chemical traps at the Pilot Fuel Enrichment Plant at Natanz (which had not begun operations at the time the samples were taken). The November 2004 report also clarifies the February 2004 revelation that 36% HEU particles had been found in two Iranian facilities – the Kalaye Electric Company (where much of Iran's centrifuge research and development had taken place) and Farayand Technique (where some centrifuge components were being made). The 36% enriched HEU particles have been found in only one room at Kalaye and on a balancing machine at Farayand (a machine which had been relocated from Kalaye); further, the agency has said that "the level of contamination suggests the presence of more than just trace quantities of material." The February 2004 report of 36% HEU samples sparked particular interest, because HEU enriched to this level is not used in Pakistan (the source of most of the centrifuge equipment), but is produced in Russia for use as fuel in certain Soviet-supplied research reactors in states in the former Soviet Union and elsewhere in the former Communist bloc. The balancing machine now at Farayand may well be the source of the 36% contamination.

Iranian special services, for smuggling of various types of nuclear or radioactive materials (though they have not been caught with substantial quantities of directly weapons-usable materials in any of the confirmed cases).[91] At the Ulba facility in Kazakhstan, canisters were found labeled for shipping to Teheran, in a room next to the room where hundreds of kilograms of HEU were located. The Iranians had reportedly approached Kazakhstan to secretly purchase beryllium and LEU from this facility, perhaps as a trust-building prelude to an offer to purchase the HEU. (The HEU was subsequently removed from this facility under the U.S.-Kazakh cooperative effort known as Project Sapphire.)[92]

If Iran succeeds in establishing an operational enrichment capability of its own, its potential demand for black market fissile material would presumably lessen. Nevertheless, as long as its enrichment facilities remained under IAEA safeguards, some demand for illicit nuclear material from abroad, which would be processed secretly without attracting inspectors' attention, might continue.

The Demand is There

There is no evidence that either a nuclear weapon or the nuclear material needed to make one has yet fallen into the hands of terrorist groups or hostile states. But it is clear that both terrorist groups and states are attempting to get these items – and that if they succeed, the international community could be faced with a terrifying new threat with very little warning. The fact that the known cases of theft and smuggling of plutonium and HEU cannot be linked to specific buyers should not blind one to the reality of the demand. Indeed, there is no way to know what has not been detected: it may be that precisely those thieves and smugglers who are well-connected to potential buyers are the ones who do not get caught.

Terrorist Nuclear Weapon Construction: How Difficult?

Mother Nature has been both kind and cruel in setting the basic parameters of the nuclear threat the world faces: kind, in that the essential ingredients of nuclear weapons – highly enriched uranium (HEU) or separated plutonium – do not exist in more than trace amounts in nature and are quite difficult to produce; cruel, in that once these materials are available, making at least a crude nuclear bomb is within the technical capability of nearly any state and potentially even some particularly capable and well-organized terrorist groups.[93]

---

[91] See, for example, "NIS Nuclear Trafficking Database" (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2006; available at http://www.nti.org/db/nistraff/ as of 12 December 2006). This database contains a large number of reported cases involving Iranian nationals. For one particularly extensive account focusing on cases in Turkey, see Ali M. Koknar, "The Trade in Materials for Weapons of Mass Destruction," *International Police Review* (March-April 1999), pp. 24-25.

[92] See discussion in William C. Potter, "Project Sapphire: U.S.-Kazakhstani Cooperation for Nonproliferation," in John M. Shields and William C. Potter, (Cambridge, Ma: Mit Press, 1997)." in *Dismantling the Cold War: U.S. And NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program*, ed. John M. Shields and William C. Potter (Cambridge, Mass.: MIT Press, 1997).

[93] This section is based on Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007). See alsoJohn P. Holdren and Matthew Bunn, "Technical Background: A Tutorial on Nuclear

This crucial fact is often not understood. As one leading analyst argued, "actually building [a crude nuclear weapon] is extremely difficult. A number of countries with vast resources and expertise, such as Iraq, have struggled unsuccessfully to produce one. It is difficult to imagine that a small terrorist group would find bomb-building any easier."[94] Unfortunately, this argument does not withstand scrutiny. Despite the failures of Aum Shinrikyo and al Qaeda to date, the capabilities needed to make a crude nuclear bomb once the nuclear material is in hand are relatively limited and could potentially be acquired by a reasonably well-organized terrorist group. The comparison to states' difficulties acquiring nuclear weapons conflates the difficulty of *producing the nuclear material* needed for a bomb – the key area on which Iraq spent billions of dollars – with the difficulty of making a bomb once the material is in hand. (As already noted, a wide range of estimates suggested that getting stolen nuclear material from abroad would have cut the time Iraq required to make a bomb from years to months.) And it fails to make the crucial distinction between making a safe, reliable, and efficient nuclear weapon suitable for delivery by a missile or a fighter aircraft – that is, the kind of nuclear weapon a typical state would want for its arsenal, whose design and construction does require substantial scientific and technical expertise – with the far simpler task of making a crude, unsafe, unreliable terrorist nuclear explosive that might be delivered by truck or boat.

If enough HEU is gathered in the same place at the same time, a nuclear chain reaction will occur. Indeed, considerable care has to be taken to prevent this from happening accidentally. To make that chain reaction explosive requires that the necessary HEU be gathered into a critical mass quickly enough, so that the material does not turn to vapor and expand enough to stop the reaction before a substantial amount of energy has been released. The bomb that obliterated the Japanese city of Hiroshima at the end of World War II was a cannon that fired a projectile of HEU into rings of HEU – a so-called "gun-type" bomb. The basic principles that need to be understood to make a gun-type bomb are widely available in the open literature.[95] Even when nothing of the kind had ever been done before, Hans Bethe, one of the technical leaders of the Manhattan Project, reports that the working principles of a gun-type bomb were "well taken care of" by one scientist and two of his graduate students during a summer study at Berkeley, before the bomb team ever arrived at Los Alamos.[96]

Gun-type weapons offer a simplicity and robustness that allows the builder to have high confidence that the weapon will perform properly without undergoing the trouble, expense, and likelihood of discovery associated with a test nuclear explosion.[97] A gun-type

---

Weapons and Nuclear-Explosive Materials," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/cnwm/overview/technical.asp as of 16 February 2006).

[94] Karl-Heinz Kamp, "Nuclear Terrorism Is Not the Core Problem," *Survival* 40, no. 4 (Winter 1998).

[95] For perhaps the best unclassified introduction, see Robert Serber, *The Los Alamos Primer: The First Lectures on How to Build an Atomic Bomb* (Berkeley: University of California Press, 1992).

[96] Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1986), p. 417.

[97] Even the makers of the *first* gun-type nuclear weapon – the four-ton "Little Boy" exploded by the United States over Hiroshima on August 6, 1945 – were confident enough of its performance to agree to its use in war without a test explosion first.

weapon, however, is highly inefficient (meaning that only a small fraction of the nuclear-explosive material used actually fissions) and so requires a substantial amount of nuclear material. The Hiroshima bomb used just over 60 kilograms of HEU metal, enriched to an average of 80% U235.[98]

It is impossible to get a substantial explosive yield from a gun-type bomb with plutonium, because the rate of spontaneous fission (primarily from Pu-240) is so high that the chain reaction will start as the two pieces in the gun get close to each other, blowing the weapon apart before any significant yield results. Hence, if the material terrorists had available was plutonium, or if the amount of HEU they had available was too small for a gun-type weapon, they would have to attempt the more challenging task of designing and building an "implosion type" weapon. An implosion type weapon uses a set of shaped explosives arranged around a less-than-critical mass of HEU or plutonium to crush the atoms of nuclear material closer together, increasing the chance that whenever one of those atoms splits and releases neutrons, those neutrons will hit and split another atom – and hence setting off the nuclear chain reaction.[99]

Designing and building an implosion bomb would be a significantly greater challenge for a terrorist group. In such a bomb, precision timing in setting off the explosives is crucial: if the explosives on one side go off much before the explosives on the other side, the nuclear material will be flattened rather than crushed to a smaller sphere, and there will be no nuclear explosion. In addition, an implosion device using either plutonium with a low Pu-240 content or HEU requires a means for generating a burst of neutrons to start the chain reaction at the right moment, before the conventional explosion destroys the configuration that will sustain a nuclear chain reaction.[100] Solving these technical challenges of implosion weapons was a major part of the Manhattan Project effort at Los Alamos during World War II. It had never been done before, and the whole approach had to be invented from scratch.[101] Today, however, with the knowledge that it can be done and substantial information on the needed explosives in the unclassified literature (explosive lenses and other shaped explosive charges are now in wide use for conventional military and even commercial applications), the challenge would be less, though still significant.

---

[98] See, for example, Carey Sublette, "Section 8.0: The First Nuclear Weapons," in *Nuclear Weapons Frequently Asked Questions* (2001; available at http://nuclearweaponarchive.org/Nwfaq/Nfaq8.html as of 12 December 2006).

[99] The Trinity and Nagasaki implosion bombs involved explosive "lenses" arranged around a six -kilogram sphere of plutonium metal (itself surrounded by a reflector), with detonators arranged all around the sphere so that the explosives were set off from every side at the same time, creating a spherical shock wave moving inward that crushed the sphere to a much higher density.

[100] In this respect, terrorists might even *prefer* to have reactor-grade plutonium, with its high Pu-240 content, than weapon-grade plutonium: because of the far larger number of neutrons released continuously by reactor-grade plutonium, an implosion bomb with this material might be able to do without a neutron generator. (This was first pointed out to the authorme by a Russian nuclear weapon designer who had been assigned to study possibilities for terrorist design and construction of a nuclear bomb.) Personal communication, February 1997.) The assured explosive yield of an implosion bomb with reactor-grade plutonium would typically be substantially lower than the yield of a device made from weapon-grade plutonium, however. See discussion in Chapter 4.

[101] See the excellent discussion in Rhodes, *The Making of the Atomic Bomb.*

Repeated examinations of the question: "could resourceful terrorists design and build a crude nuclear bomb if they had the needed nuclear material?" by nuclear weapons experts in the United States and elsewhere have concluded that the answer is "yes" – for either type of nuclear bomb.[102] A detailed examination by the U.S. Office of Technology Assessment, drawing on all the relevant classified information, summed up the situation in a conclusory statement intended to apply to both gun-type and implosion-type devices:

> A small group of people, none of whom have ever had access to the classified literature, could possibly design and build a crude nuclear explosive device. They would not necessarily require a great deal of technological equipment or have to undertake any experiments. Only modest machine-shop facilities that could be contracted for without arousing suspicion would be required. The financial resources for the acquisition of necessary equipment on open markets need not exceed a fraction of a million dollars. The group would have to include, at a minimum, a person capable of researching and understanding the literature in several fields and a jack-of-all trades technician.[103]

Setting off a nuclear explosion with HEU can be done rapidly enough that U.S. Department of Energy (DOE) internal security regulations require that security for U.S. nuclear sites where enough material for a bomb is present be based on keeping terrorists out entirely, rather than catching them as they leave the site, to avoid "an unauthorized opportunity...to use available nuclear materials for onsite assembly of an improvised nuclear device" – that is, to prevent terrorists from being able to set off a nuclear explosion while they were still inside the facility where they stole the HEU.[104]

Given the importance of the question of whether terrorists could design a nuclear explosive, the answer has not been left to analysis alone, but has been subjected to "experiment" as well. In 1977, a Princeton undergraduate designed an implosion-type bomb

---

[102] See J. Carson Mark et al., "Can Terrorists Build Nuclear Weapons?" in *Preventing Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Lexington, Mass: Lexington Books, 1987; available at http://www.nci.org/k-m/makeab.htm as of 4 January 2006). This remains the most authoritative unclassified treatment of the subject – in part because it represents something of a negotiated statement by experts with a range of views on the matter.

[103] U.S. Congress, Office of Technology Assessment, *Nuclear Proliferation and Safeguards* (Washington, D.C.: OTA, 1977; available at http://www.wws.princeton.edu/ota/disk3/1977/7705/7705.PDF as of 12 December 2006), p. 140. A million 1977 dollars would be approximately $2.8 million in 2007 dollars. This report does, however, argue that under-appreciated difficulties of actually fabricating a gun-type device would make doing so essentially as difficult as designing and building an implosion bomb. After consulting with a number of nuclear weapon designers, I strongly disagree, at least with respect to a crude terrorist gun-type device that would not require high reliability or efficiency. The relative difficulty of gun-type and implosion-type devices is discussed in more detail in Chapter 4.

[104] U.S. Department of Energy, Office of Security Affairs, Office of Safeguards and Security, *Manual for Protection and Control of Safeguards and Security Interests*, DOE-M-5632.1c-1 (Washington, D.C.: DOE, 1994; available at http://www.fas.org/irp/doddir/doe/m5632_1c-1/index.html as of 28 February 2006). This order has now been superceded, and more recent orders are either less explicit or not publicly available. In fact, however, the use of a denial strategy, because of concerns that terrorists might be able to use materials readily to hand to make an improvised nuclear device, has been expanded at DOE since 9/11. See discussion in U.S. Congress, Government Accountability Office, *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat* (GAO, 200423 December 2006), p. 12.

for a senior paper; Freeman Dyson, a veteran of post-war nuclear weapon design work who was his professor, gave him an "A" on the paper, and the government then classified it.[105] Of the several official investigations of this kind that have occurred, two have been revealed publicly in some detail. In one effort in the 1960s (before the availability of the Internet or of a large fraction of the information that is unclassified and readily available today), two physicists who had just received their doctorates and had no knowledge of weapons-usable nuclear materials, nuclear weapons, or explosives were given the job of using unclassified information to design a nuclear bomb from scratch. (There were ultimately a total of three participants, as one of the original two dropped out and was replaced.) They quickly decided that designing a workable gun-type bomb would be too easy to show off their technical skills in a way that would improve their subsequent job prospects; instead, they successfully designed a workable implosion design. Two points about this effort should be noted, however: (a) since this experiment was intended to assess the capabilities of states, rather than terrorist groups, the team had the opportunity to carry out "experiments" in which they wrote up what they wanted to test (such as different explosive arrangements), and the experts overseeing the effort told them what the result of such a test would be (an option that would not be available for terrorist groups seeking to avoid detection); (b) they only designed the weapon, they did not manufacture it.[106]

More recently, Senator Joseph Biden (D-DE), when serving as chairman of the Senate Foreign Relations Committee, asked the three U.S. nuclear weapons laboratories whether terrorists, if they had the nuclear material, could make a crude but workable nuclear bomb. The answer given was "yes." Senator Biden reports that within a few months after he had asked the question, the laboratories had actually built a gun-type device, using only components that, except for the nuclear material itself, were off the shelf and commercially available without breaking any laws. The device was actually brought into a secure Senate hearing room to demonstrate the gravity of the threat.[107]

The process of actually making the bomb would require some expertise and equipment (though all of the equipment needed is commercially available). Casting and machining the uranium or plutonium parts for a bomb would be a significant challenge, unless the group managed to acquire nuclear material in readily usable form, or included people with experience in uranium or plutonium metallurgy. For a gun-type bomb, the group would need to understand cannon ballistics. For an implosion bomb, figuring out how to detonate the explosives at multiple points with the level of timing precision required would be a challenge.

---

[105] John Aristotle Phillips and David Michaelis, *Mushroom: The Story of the a-Bomb Kid*, 1st ed. (New York: Morrow, 1978).

[106] See Dan Stober, "No Experience Necessary," *Bulletin of the Atomic Scientists* 59, no. 2 (2003; available at http://www.thebulletin.org/article.php?art_ofn=ma03stober as of 27 February 2006). Expurgated declassified documents describing the effort are also available at the same site.

[107] Joseph Biden, "Avoiding Nuclear Anarchy," in *The Paul C. Warnke Conference on the Past, Present, and Future of Arms Control, Georgetown University, Washington, D.C.*, (Washington, D.C.: Arms Control Association, Edmund A. Walsh School of Foreign Service, and Center for Peace and Security Studies, 2004; available at http://www.armscontrol.org/PDF/WarnkePDFTranscript.pdf as of 12 December 2006).

Making a nuclear bomb would not be easy for a terrorist group; but these challenges are far from insuperable.

Having help from someone familiar with nuclear weapon design and construction would certainly be useful to terrorists trying to build a bomb – as would having actual bomb blueprints – though neither would be essential. As noted earlier, Al Qaeda and its allies have actively attempted to recruit such help, from Pakistani nuclear scientists and, it appears, from Russian scientists as well.

Over the last several years, the world has seen confirmed an extraordinary leakage of nuclear technology from Pakistan, including designs for uranium enrichment centrifuges, components for such centrifuges, complete centrifuges apparently taken from Pakistan's own enrichment plant, consulting services for any problems the buyers might have, and even actual nuclear weapon blueprints. The leakers were apparently motivated both by money and by Islamic fervor.[108] Extreme Islamic views, including sympathy for al Qaeda and the Taliban, appear not to be unusual in Pakistan's military and nuclear establishment, just as they are not unusual in broader Pakistani society. A.Q. Khan, the former head of Pakistan's nuclear weapons program who confessed to leading this clandestine nuclear network, is a strident nationalist prone to harsh Islamic rhetoric. In 1984 (three years before Iran now says it received complete centrifuge designs), Khan spoke of his opposition to "all the Western countries" as "enemies of Islam," and the possibility that nuclear technology might be shared among Islamic countries, specifically mentioning Iraq, Libya, and Iran:

> All the Western countries, including Israel, are not only Pakistan's enemies but also enemies of Islam. ...All this is part of the Crusades, which the Christians and Jews had initiated against the Moslems 1000 years ago. Islam was the only religion which uprooted their culture and civilization and they have not forgotten it even today. ...All countries are aware that Moslems believe in monotheism and despite political disunity, they share each other's hardships. They are afraid that if Pakistan makes obvious progress in this field, then the whole Islamic world will stand to benefit. There is no such danger from India. You know that Iraq, Libya and Iran had increased ties with India in the hope that India would assist them in nuclear technology but this was not the case and they were

---

[108] Good summaries of the Khan network can be found in Chaim Braun and Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime," *International Security* 29, no. 2 (Fall 2004; available at http://iis-db.stanford.edu/pubs/20716/braun-chyba-is-fall04.pdf as of 1 August 2005); David Albright and Corey Hinderstein, "Unraveling the A.Q. Khan and Future Proliferation Networks," *Washington Quarterly* 28, no. 2 (Spring 2005; available at http://www.twq.com/05spring/docs/05spring_albright.pdf as of 1 August 2005); Barton Gellman and Dafna Linzer, "Unprecedented Peril Forces Tough Calls; President Faces a Multi-Front Battle against Threats Known, Unknown," *Washington Post*, 26 October 2004; Bill Powell et al., "The Man Who Sold the Bomb," *Time* 165 (21 February 2005), p. 22; Douglas Frantz, "A High-Risk Nuclear Stakeout: The U.S. Took Too Long to Act, Some Experts Say, Letting a Pakistani Scientist Sell Illicit Technology Well after It Knew of His Operation," *Los Angeles Times*, 27 February 2005; William C. Rempel and Douglas Frantz, "Global Nuclear Inquiry Stalls: Authorities Fear That the Extent of a Pakistani Scientist's Proliferation Ring Remains Unknown and That It Will Resume Work If Pressures Ease," *Los Angeles Times*, 5 December 2004; John Lancaster and Kamran Khan, "Pakistani Scientist Apologizes; Nuclear Assistance Unauthorized, He Says," *Washington Post*, 5 February 2004.

sorely disappointed. This is the reason why Western countries ignore India's nuclear program and its results and are after us. [109]

In 1998, when the United States bombed al Qaeda camps in Afghanistan in retaliation for the bombings of U.S. embassies in Africa, General Aslam Beg, who until shortly before had been in overall charge of Pakistan's nuclear program, told reporters that "by the grace of God" bin Laden had not been in the bombed camps and therefore had not been killed. [110] Beg is so powerful even in retirement that he openly told reporters during the ongoing investigation of nuclear leakage in Pakistan that Pakistani official investigators "would not dare" even question him – repeating it a second time for emphasis.[111] One Pakistani nuclear physicist critical of Pakistan's nuclear weapons programs has estimated that some 10 percent of Pakistan's nuclear experts – amounting to hundreds of people – hold extremist Islamic views that could motivate nuclear leakage.[112]

Not only scientific help but actual working bomb designs now appear to be potentially available, moreover. Libya, in its decision to roll back its weapons of mass destruction programs, has admitted receiving an implosion design that appears to have come from Pakistan (though it appears to have originated in China, which apparently provided it to Pakistan long ago). The copy of the design that Libya acknowledged has been removed from Libya – but who knows how many other copies exist, where they have gone, and where they may go in the future? The possibility that al Qaeda has access to complete blueprints for an implosion-type nuclear explosive – or may soon get such access – is very real. The design is reportedly one for a relatively simple and not very efficient implosion bomb – the type of implosion weapon that terrorists could most plausibly manufacture.[113]

Of course, even with a working design, and even if the nuclear material could be acquired, manufacturing a weapon to the specifications called for in the design would not be a trivial task. But the potential availability of a nuclear bomb recipe reinforces the urgency of keeping the ingredients needed to make that recipe out of terrorist hands.

---

[109] "Exclusive Interview with Dr. Abdul Qadeer Khan (Excerpts)," trans. BBC Summary of World Broadcasts, *Nawa-e Waqt*, 10 February 1984.

[110] Elizabeth Neuffer, "A US Concern: Pakistan's Arsenal: Anti-American Mood Poses a Security Risk," *Boston Globe* 2002.

[111] Quoted in David Rohde, "General Denies Letting Secrets of a-Bomb out of Pakistan," *New York Times*, 27 January 2004.

[112] Neuffer, "A US Concern: Pakistan's Arsenal: Anti-American Mood Poses a Security Risk." For further discussion of the problem of extreme Islamic views in Pakistan's nuclear establishment, see Albright and Higgins, "A Bomb for the Ummah."

[113] William J. Broad, "Libya's Crude Bomb Design Eases Western Experts' Fear," *New York Times*, 9 February 2004. The design has been widely reported as being the warhead for the Chinese DF-2, the first missile-delivered Chinese warhead. David Albright and Corey Hinderstein describe the design recovered in Libya as a Chinese missile-warhead design weighing approximately 500 kilograms. Albright and Hinderstein, "Unraveling the A.Q. Khan and Future Proliferation Networks."

Could Terrorists Produce Their Own Bomb Material?

Revelations that Pakistani nuclear scientist Abdul Qadeer Khan and his co-conspirators had organized a far-flung nuclear black market that had supplied complete uranium enrichment centrifuges to Libya, Iran, and apparently North Korea have raised questions about whether access to such technology might allow even a terrorist group to produce highly enriched uranium (HEU) or plutonium for itself, rather than having to rely on obtaining already produced material from a state that already possesses it. The Japanese terror cult Aum Shinrikyo apparently planned to try, having purchased a farm in Australia for its uranium deposits, and stolen documents relating to laser isotope enrichment.

To produce HEU first requires mining or obtaining uranium ore, converting that ore into a chemical form suitable for enrichment, and then enriching it – concentrating the isotope U-235, which is less than 1% of the uranium that occurs naturally, to at least (and likely far above) the 20 percent concentration defined as HEU. A variety of enrichment technologies exist, each posing difficult obstacles. The Khan network was peddling centrifuge technology, which uses sets of hundreds or thousands of sophisticated, ultra-high-speed, spinning centrifuges to separate U-235 from the slightly heavier U-238. But even with complete centrifuges provided from the black market, building and operating an enrichment facility would be extraordinarily difficult for a terrorist group. Iran, for example, is a nation with a strong indigenous science and technology base and substantial monetary resources, and Iran now admits that it received complete centrifuge designs as early as 1987. Yet for years thereafter, the Iranian enrichment program apparently made little progress. Although Iran received an additional infusion of help from the network in the mid-1990s, a decade after that second infusion of help Iran appears only now to be at the cusp of mastering the technology to build its own centrifuges and operate them in effective enrichment cascades.[114]

If a terrorist group had access to a substantial quantity of low-enriched uranium (LEU), and was willing to leave a substantial fraction of the U-235 in the LEU in the depleted tails from the enrichment operation, the amount of enrichment work required to make bomb material might be reduced by 80-90 percent. Getting that enrichment work done, however, would still pose an immense challenge – though analysts from the Kurchatov Institute in Moscow in particular have warned that for a much smaller amount of enrichment work, much lower-quality centrifuges that might be easier to acquire and operate might be used.[115] A good case can be made, based on the Kurchatov analysis and others, that more stringent global controls should be imposed on LEU than now exist – especially given the danger of its use for covert proliferation by a state. But even with LEU, actually operating an enrichment enterprise sufficient to make a bomb's worth of HEU would be far more difficult for a terrorist group to accomplish than making a bomb from stolen nuclear material; it is difficult to imagine any of the terrorist groups the world has yet seen coming close to mastering the challenge of enrichment.

---

[114] Albright and Hinderstein, "Iran's Next Steps".

[115] Alexander Rumiantsev, Vladimir Sukhoruchkin, and Vladimir Schmelev, personal communication, October 2005.

For terrorists to produce their own plutonium would require either (a) building a nuclear reactor to produce plutonium in spent fuel or (b) getting stolen spent fuel. In either case, the group would then need to build at least a crude facility to extract plutonium from the spent fuel. Building a plutonium production reactor, operating it long enough to produce a bomb's worth of plutonium, and then separating that plutonium from the reactor's spent fuel appear to be a set of activities well beyond the capabilities of any terrorist group known to date; it is extremely unlikely any terrorist group will develop such capabilities in the future. Managing to separate plutonium from stolen spent fuel is somewhat more plausible, as a crude facility for that purpose need not be very large, and could be built with technologies that are commercially available, relying on chemical processes that have been openly published. But spent power reactor fuel is massive and intensely radioactive, making it very difficult to steal. Processing the material in the presence of its intense radioactivity is much more difficult than processing unirradiated fuel, because of the requirement to handle the various operations remotely, and the difficulty of fixing any problems that may arise in the presence of the intense radiation field that exists once the facility has begun to be used. The terrorists would have to reckon with a significant probability that the vehicle carrying the intensely radioactive material away from the theft site – which would be substantially easier to detect with radiation sensors than a truck carrying unirradiated plutonium or HEU – would be found and stopped, or that their facility for separation (also more detectable than it would be with less radioactive material) would be found and destroyed before it could finish its work.

In short, even given the leakage of technology from the Khan network, it appears extremely unlikely that terrorist groups will develop the capacity to produce their own nuclear bomb material. If the stockpiles of nuclear weapons and weapons-usable materials held by states can be secured reliably and kept out of terrorist hands, the probability of nuclear terrorism can be reduced to a very low level.

Setting Off a Stolen Nuclear Weapon

A terrorist group that got hold of a stolen nuclear weapon would face somewhat different challenges than would a group trying to make a bomb of its own from stolen nuclear material. The difficulty of setting off a stolen weapon would depend substantially on the specifics of the weapon's design. Many U.S. nuclear weapons are equipped with "permissive action links" (PALs), which are effectively electronic locks, intended to make it difficult to detonate the weapon without first inserting an authorized code. Modern versions are designed to be integral to the weapon, making it very difficult to bypass the locking device and "hotwire" the weapon to detonate. They are also equipped with "limited try" features that will permanently disable the weapon if the wrong code is entered too many times, or if attempts are made to tamper with or bypass the lock.[116] Older versions do not have all of

[116] For discussions of PALs and their role, see, for example, Peter Stein and Peter Feaver, *Assuring Control of Nuclear Weapons: The Evolution of Permissive Action Links*, Csia Occasional Paper, No. 2 (Cambridge, Mass.: Center for Science and International Affairs, Harvard University, 1987); Peter Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, N.Y.: Cornell University Press, 1992); Donald R. Cotter, "Peacetime Operations: Safety and Security," in *Managing Nuclear Operations*, ed. Ashton B. Carter, Charles A. Zraket, and John D. Steinbruner (Washington, D.C.: Brookings Institution, 1987).

these features and therefore would provide somewhat less of an obstacle to a terrorist group attempting to detonate a stolen weapon they had acquired.

In addition to PALs, for safety reasons many weapons are equipped with devices which prevent the weapon from detonating until it has gone through its expected flight-to-target sequence – for example, in the case of a nuclear artillery shell, the explosive acceleration of being fired from a cannon, followed by the coasting through the air of unpowered flight. These features, if designed to be very difficult to bypass, can also pose a serious obstacle to a terrorist group detonating a stolen weapon.[117]

Unfortunately, what little information is publicly available suggests that older Soviet-designed weapons, particularly older tactical weapons, may not be equipped with modern versions of such safeguards against unauthorized use.[118] In both the United States and Russia, thousands of nuclear weapons, particularly older varieties, have been dismantled in recent years, and it is likely that most of the most dangerous weapons lacking modern safeguards have been destroyed. But neither country has made any commitment to destroy all of these weapons. Nuclear powers such as Pakistan, India, and China are not believed to incorporate equivalents to modern PALs in their weapons, but many of these weapons are believed to be stored in partly disassessembled form.

Perhaps even more than in building a crude nuclear device of their own, terrorists seeking to detonate a stolen weapon would benefit greatly from the help of a knowledgeable insider, if such help could be procured. It may well be that an insider willing to help in stealing a weapon in the first place might also be willing to help in providing important information related to setting the weapon off. In the case of a weapon equipped with a modern PAL, however, without the actual use codes most insiders, too, would not be able to provide ready means to overcome the lock and use the weapon. (After all, a principal purpose of PALs is to prevent insiders from being able to set the weapons off without authorization.)

If they could not figure out how to detonate a stolen weapon, terrorists might choose to remove the nuclear material from it and seek to fashion it into a bomb – though if the weapon was a modern, highly efficient design using a modest amount of nuclear material, the material contained in it might not be enough for a crude, inefficient terrorist bomb.[119] In any

---

[117] For a description of such "environmental sensing devices" (ESDs), see, for example, Cotter, "Peacetime Operations: Safety and Security."

[118] See, for example, testimony of Bruce G. Blair in National Security Committee, Military Research & Development Subcommittee, *Hearing on Russian Missile Detargeting and Nuclear Doctrine and Its Relation to National Missile Defense*, U.S. House of Representatives, 105th Congress, 1st Session, 13 March 1997 (available at http://armedservices.house.gov/testimony/105thcongress/97-3-13Blair.htm as of 28 February 2006). Blair reports that tactical nuclear weapons "built before the early 1980s lack the safety locks known as permissive action links." See also Bruce W. Nelan, "Present Danger: Russia's Nuclear Forces Are Sliding into Disrepair and Even Moscow Is Worried About What Might Happen," *Time Europe* 149, no. 14 (7 April 1997), p. 42. Nelan reports U.S. intelligence estimates that Russian tactical weapons "often" have external locks "that can be removed, and many have none at all."

[119] If the weapon were a multi-stage thermonuclear weapon, it would be more likely to have sufficient nuclear material for a crude terrorist bomb. Such weapons include a "primary" or "pit", which uses plutonium or HEU to create an initial nuclear blast, and the energy from that blast causes fusion to occur in the "secondary," which typically also includes HEU, in which additional fission occurs. Combining material from the two parts of the

case, terrorists who had a stolen nuclear weapon would be in a position to make fearsome threats – for no one would know for sure whether they could set it off or not.

How Much Do Al Qaeda's Weaknesses Reduce the Danger?

Several weaknesses of al Qaeda have led some analysts to argue that it could not plausibly carry out an attack with an actual nuclear explosive. First, many of the organization's recruits have little technical sophistication and expertise. For example, a 1999 al Qaeda progress report found in Afghanistan concludes that the attempt to make nerve gas weapons relying on the expertise the group could put together without recruiting specialists had "resulted in a waste of effort and money." The report recommended recruiting experts as the "fastest, cheapest, and safest" way to build the capability to make such weapons.[120] Unfortunately, however, a number of top al Qaeda personnel are technologically literate (bin Laden deputy Zawahiri is a medical doctor, while reported 9/11 mastermind Khalid Sheikh Muhammad, now in U.S. custody, is a U.S.-trained engineer),[121] and they may well have succeeded in recruiting other technically skilled individuals who are as yet unknown. Despite the limited public evidence that suggests a lack of sophistication in their nuclear efforts to date, the group has demonstrated a significant ability to carry out research on technical subjects in the unclassified literature.[122] The most detailed unclassified analysis of al Qaeda's nuclear program concludes that it posed a serious threat while it was underway in the Afghanistan sanctuary and could still succeed elsewhere.[123]

Others argue that a group with al Qaeda's structure of small cells would not be well-suited for what they argue would be a large, long-term project like making a nuclear bomb – particularly given the substantial disruptions al Qaeda has suffered from the international response to the 9/11 attacks. The deaths or arrests of a substantial number of senior al Qaeda leaders and operatives since 9/11 and the other disruptions of its operations have undoubtedly reduced the probability of al Qaeda succeeding in pulling off a nuclear explosive attack. But the crucial question is: by how much? Unfortunately, as already noted, the conclusion of repeated technical studies is that the group needed to design and fabricate a crude nuclear explosive, once the needed materials were in hand, might be quite small – as small as a single al Qaeda cell. The ability of a cell-based organization like al Qaeda – or even one of the many loosely affiliated regional groups that now appear to be posing an increasing threat as

---

weapon would make it more likely that a bomb would have enough material for a crude terrorist bomb. It is not likely, however, that a single stolen weapon would have enough HEU for a gun-type bomb, unless it was itself a gun-type bomb.

[120] Alan Cullison and Andrew Higgins, "Files Found: A Computer in Kabul Yields a Chilling Array of Al Qaeda Memos," *The Wall Street Journal*, 31 December 2001.

[121] See, for example, National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, p. 146.

[122] For an account of al Qaeda's extensive research in the unclassified literature on biological weapons gleaned from materials recovered from al Qaeda safehouses in Afghanistan, see James B. Petro and David A. Relman, "Understanding Threats to Scientific Openness," *Science* 302, no. 5652 (12 December 2003). Supplementary on-line material includes a list of biological warfare references put together by al Qaeda experts.

[123] Albright, "Al Qaeda's Nuclear Program."

the old central structure of al Qaeda is weakened – to make a crude nuclear explosive cannot be dismissed.

Similarly, some argue that in the absence of a stable sanctuary where a technical development effort could be undertaken over a substantial period of time, with large fixed facilities, it would be nearly impossible for a terrorist group to make a nuclear bomb – and that therefore the destruction of the Afghanistan sanctuary makes any nuclear attack by al Qaeda extremely unlikely.

The overthrow of the Taliban regime and the removal of al Qaeda's sanctuary in Afghanistan undoubtedly disrupted al Qaeda's nuclear efforts significantly. But two crucial points should be made. First, as noted earlier, large fixed facilities are not necessarily required for putting together a crude nuclear explosive, and the time required may be short (as suggested by the DOE regulation warning against the possibility of nuclear explosives being made while a terrorist group was still inside a building where they had stolen nuclear material). The building that South Africa used to assemble its nuclear weapons is a very ordinary-looking warehouse, with little external sign of the deadly activities that went on inside.[124] The world's first nuclear bomb, for the Trinity test, was put together in a small area at the base of a tower; the bomb was then lifted to the top of the tower with cables (with a truckload of mattresses underneath in case the bomb fell).[125] Testing of gun designs for the Hiroshima bomb was accomplished by firing projectiles into a pile of sand.[126] Terrorist processing of nuclear material and manufacture of a crude nuclear bomb might well be done on the premises of an apparently legitimate front company or at an isolated location in a developed country.[127] In short, there is no reason to be confident that the facilities and activities needed to make a bomb would be noticed before it was too late.

Second, a wide range of possible sanctuaries still exist – from the mountains on both sides of the Afghan border, to failed states such as Somalia, to remote jungle and desert areas around the world, where it is believed new terrorist bases are being established. Indeed, in March 2004, CIA Director Tenet told the Senate Select Committee on Intelligence of his

---

[124] See discussion of "the Circle" building where South Africa's gun-type bombs were assembled after the program was transferred to Armscor, in David Albright, "South Africa and the Affordable Bomb," *Bulletin of the Atomic Scientists* 50, no. 4 (1994; available at http://www.thebulletin.org/article.php?art_ofn=ja94albright as of 28 February 2006). The weapons were assembled on the first floor of the building, which had approximately 4,000 meters of floorspace. South Africa consciously avoided equipping the building with features that would have made its importance obvious – such as high-technology satellite communications on the roof. The only distinguishing feature of the building is an earth embankment on one side, intended to block the building from view from the road within a large Armscor site.

[125] For a discussion and a photograph of the small group assembling the bomb, see Lillian Hoddeson et al., *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945* (Cambridge, UK: Cambridge University Press, 1993), pp. 367-370.

[126] For a discussion of initial testing of projectiles and targets for the gun, see Hoddeson et al., *Critical Assembly*, pp. 116-119. A piece of cardboard in front of the gun, which the projectiles passed through, leaving a hole behind, was used to measure the projectiles' deviation from their intended path.

[127] For a description of a scenario in which this activity might take place within the United States itself, see Peter D. Zimmerman and Jeffrey G. Lewis, "The Bomb in the Backyard," *Foreign Policy*, no. 157 (November/December 2006), pp. 32-39.

concern for the number of areas around the world where central governments have no consistent reach: "We count approximately 50 countries that have such 'stateless zones.' In half of these, terrorist groups are thriving."[128]

The bottom line, unfortunately, is that if a sophisticated terrorist group got a stolen nuclear bomb or enough nuclear material to make one, there can be few grounds for confidence that they would be unable to use it.

Size and Distribution of Global Nuclear Stockpiles

An important element of the threat of nuclear theft is the massive size and broad distribution of the global stockpiles of nuclear weapons and the materials needed to make them.

Today, more than a decade after the end of the Cold War, there are still more than 25,000 assembled nuclear weapons in the world.[129] While Russia and the United States own some 95% of these weapons, nine countries possess such weapons (assuming that North Korea's statements that it has manufactured nuclear weapons beyond the one tested in 2006 are accurate). The five states with the largest number of nuclear weapons are the five nuclear-weapon state parties to the Nonproliferation Treaty (NPT): Russia, the United States, China, France, and the United Kingdom. The four other states with nuclear weapons are the only states outside the NPT, India, Pakistan, Israel, and North Korea. (North Korea is the only country to have joined the treaty and then withdrawn.) See Table 2.1. In addition to these nine countries that possess nuclear weapons of their own, U.S. nuclear weapons are reportedly located in six other countries – one other nuclear weapon state (the United Kingdom) and five non-nuclear-weapon states (Germany, the Netherlands, Belgium, Italy, and Turkey).[130]

---

[128] *Worldwide Threats.*

[129] This includes an estimated 16,000 remaining in Russia's stockpiles; over 10,000 remaining in the U.S. nuclear stockpiles; and over 1,000 warheads in the combined total of other countries' stockpiles. See Robert S. Norris and Hans S. Kristensen, "NRDC Nuclear Notebook: Global Nuclear Stockpiles, 1945-2006," *Bulletin of the Atomic Scientists* 62, no. 4 (July/August 2006; available at http://www.thebulletin.org/article_nn.php?art_ofn=ja06norris as of 13 August 2006), pp. 64-66.

[130] As a result of the 1991 Presidential Nuclear Initiatives, U.S. nuclear weapons have been removed from South Korea and from surface ships, which previously regularly carried them to countries around the world. The deployments in Europe, and on submarines, are believed to be the only remaining U.S. nuclear weapons deployments beyond U.S. shores. For a detailed discussion of the remaining U.S. nuclear weapons in Europe, see Hans M. Kristensen, *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning* (Washington, D.C.: Natural Resources Defense Council, 2005; available at http://www.nrdc.org/nuclear/euro/euro.pdf as of 19 July 2005).

Table 2.1: World Stockpiles of Nuclear Weapons

Country	# weapons	% of world
Russia	16,000	58.91%
United States	10,100	37.19%
China	200	0.74%
France	350	1.29%
United Kingdom	200	0.74%
Israel	150	0.55%
India	85	0.31%
Pakistan	70	0.26%
North Korea	6	0.02%
Total	27,161	100.00%

Sources: For Russia, the United States, Britain, France, and China, see Robert S. Norris and Hans M. Kristensen, "NRDC Nuclear Notebook: Global Nuclear Stockpiles 1945-2006," *Bulletin of the Atomic Scientists* 62 no. 4 (July/August 2006; available at http://www.thebulletin.org/article_nn.php?art_ofn=ja06norris as of 2 January 2007). (I have rounded their figure for the United States to the nearest hundred.) For Israel, the figure in the table is a rounding of the midpoint of the range given in Robert S. Norris, William Arkin, Hans M. Kristensen, and Joshua Handler, "NRDC Nuclear Notebook: Israeli Nuclear Forces, 2002," *Bulletin of the Atomic Scientists* (September/October 2002; available at http://www.thebulletin.org/article_nn.php?art_ofn=so02norris as of 2 January 2007); more recently, in "Global Nuclear Stockpiles 1945-2006," Norris and Kristensen report that the U.S. Defense Intelligence Agency estimates Israel's arsenal at 60-85 warheads. For India and Pakistan, the figures here represent an assumption that nearly all the military plutonium and HEU on hand has been incorporated into weapons; the estimates in the table are the mid-range of the estimates in Institute for Science and International Security, "India" (2004; available at http://www.isis-online.org/mapproject/country_pages/india.html as of 2 January 2007); and Institute for Science and International Security, "Pakistan" (2004; available at http://www.isis-online.org/mapproject/country_pages/pakistan.html as of 2 January 2007); similarly, Norris and Kristensen, in "Global Nuclar Stockpiles 1945-2006," estimate that "India and Pakistan have about 110 nuclear warheads between them." For North Korea, the figure in the table assumes that roughly six kilograms of plutonium are required for one bomb, that all available separated plutonium has been fabricated into weapons, and that the total available plutonium is roughly in the middle of the range of 20-53 kilograms reported in David Albright and Paul Brannan, "The North Korean Plutonium Stock, Mid-2006" (Washington, D.C.: Institute for Science and International Security, 2006; available at http://www.isis-online.org/publications/dprk/dprkplutonium.pdf as of 13 August 2006).

World stockpiles of separated plutonium and HEU, the essential ingredients of nuclear weapons, amount to well over 2,300 tons – enough to manufacture over 200,000 nuclear weapons.[131] Neither of these materials occurs in significant quantities in nature; these

[131] These figures include only plutonium separated from spent fuel, not the larger amount of plutonium in spent fuel. They include the plutonium and HEU in intact weapons and their components, as well as additional material stored in a wide range of other forms (the largest categories being metals and oxides); the plutonium figure includes both separated plutonium in military stockpiles and separated "reactor-grade" plutonium in civilian stockpiles, both of which are usable in nuclear explosives. (The weapons-usability of reactor-grade plutonium is discussed in detail in Chapter 4.) They include also plutonium and HEU in fabricated fuel elements;

stockpiles of weapons and materials have all been consciously produced by human beings in the first six decades of the nuclear age.

Unlike nuclear weapons, separated plutonium and HEU have both military and civilian uses. A number of countries reprocess plutonium from spent fuel and recycle it as plutonium-uranium mixed oxide (MOX) fuel in civilian reactors, resulting in the processing, transport, and use of many tons of weapons-usable separated plutonium every year. In recent years, use of the separated plutonium as fuel has not kept pace with reprocessing, with the result that as of the end of 2003, nearly 240 tons of separated, weapons-usable plutonium existed in civilian stockpiles worldwide – a figure that will soon surpass the total amount of separated plutonium in all the world's nuclear weapon stockpiles.[132]

---

the definition used to determine what should be included is almost the same as the International Atomic Energy Agency's definition of "unirradiated direct use material" – that is, all materials containing plutonium and HEU which do not emit more than 100 rem/hr at 1 meter and are not "practically irrecoverable." International Atomic Energy Agency, *IAEA Safeguards Glossary* (Vienna: IAEA, 2001; available at http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/Start.pdf as of 19 July 2005). The difference from that definition is that no attempt has been made in these figures to exclude civil HEU emitting more than 100 rem/hr at 1 meter; as discussed in Chapter 4, the overwhelming majority of that material is not emitting sufficient radiation to greatly reduce the proliferation concerns it poses. These figures are from David Albright and Kimberly Kramer, eds., *Global Fissile Material Inventories* (Washington, D.C.: Institute for Science and International Security, 2004; available at http://www.isis-online.org/global_stocks/tableofcontents.html as of 14 February 2005). These figures are updates of the detailed review of these stockpiles provided in David Albright, Frans Berkhout, and William B. Walker, *Plutonium and Highly Enriched Uranium, 1996: World Inventories, Capabilities, and Policies* (Solna, Sweden; Oxford, UK; and New York: Stockholm International Peace Research Institute (SIPRI) and Oxford University Press, 1996). The HEU figures are for tons of 90% enriched equivalent, so if, for example, a country had two tons of 45% enriched material, that would count as one ton in these estimates. The U.S. Department of Energy has officially declassified the fact that it is theoretically possible to make a bomb from four kilograms of weapon-grade plutonium, and that figure is used here for calculating the bomb equivalents for military stocks. See U.S. Department of Energy, *Restricted Data Declassification Decisions 1946 to the Present (RDD-7)* (Washington, D.C.: DOE, 2001; available at http://www.fas.org/sgp/othergov/doe/rdd-7.html as of 14 August 2006). The higher isotopes of plutonium present in reactor-grade plutonium have larger critical masses, so five kilograms is used for calculating bomb equivalents for civilian plutonium stockpiles. The quantity of HEU required, at a 90% enrichment level, is often taken to be 2.5-3 times the needed quantity of plutonium; to be sure not to overstate the case, we have used 15 kilograms of HEU for the bomb equivalent estimate here (3.75 times the plutonium figure used). These figures are for implosion-type devices. Unclassified analyses suggest that in principle, with good designs it is possible to make nuclear explosives with substantially less material than envisioned in the weapons-equivalent figures used here. See Thomas Cochran and Christopher Paine, "The Amount of Plutonium and Highly-Enriched Uranium Needed for Pure Fission Nuclear Weapons" (Washington, D.C.: Natural Resources Defense Council, 13 April 1995; available at http://www.nrdc.org/nuclear/fissionw/fissionweapons.pdf as of 19 July 2005). It is also important to note that modern thermonuclear weapons typically have nuclear material both in the fissionable core of the weapon (known as the "primary" or "pit") and in the thermonuclear portion (known as the "secondary"), and thus the average total amount of weapons-usable nuclear material per weapon in the stockpiles of the major nuclear weapon states is substantially more than the figures used in these weapon-equivalents figures.

[132] See David Albright and Kimberly Kramer, "Plutonium Watch: Tracking Civil Plutonium Inventories," in *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, 2005; available at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html as of 21 July 2005).

HEU is no longer used in civilian power reactors (with a couple of exceptions), but remains widely used in civilian research reactors (as well as for medical isotope production, in naval and icebreaker reactors, as spike fuel in plutonium and tritium production reactors, and for some other purposes). Over 130 research reactors in some 40 countries continue to operate with HEU as their fuel.[133]

Some of these do not have enough nuclear material on-site for a bomb, but many do – as do many associated facilities, such as fuel fabrication plants. All told, there are an estimated 128 research reactors or associated facilities worldwide that possess at least 20 kilograms of HEU.[134] Of these, 41 are fuel facilities rather than research reactors themselves.[135] There are an estimated 65 tons of HEU in civilian use worldwide.[136] As a result, while nearly half of the estimated world stockpile of nearly 490 tons of separated plutonium at the end of 2003 was civilian, only about 3% of the estimated world stockpile of HEU was civilian. See Figure 2.1 and Figure 2.2.

---

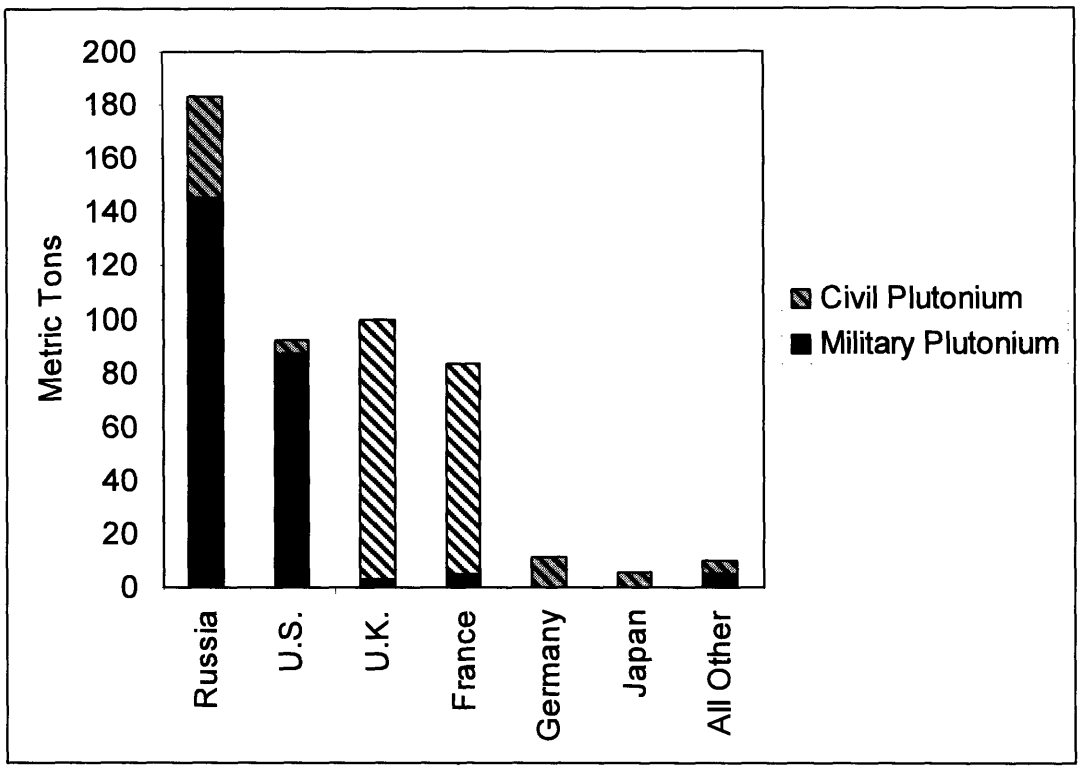
[133] See, for example, the data provided in U.S. Congress, Government Accountability Office, *Nuclear Nonproliferation: DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium in Civilian Research Reactors*, GAO-04-807 (Washington, D.C.: GAO, 2004; available at http://www.gao.gov/new.items/d04807.pdf as of 2 February 2005). GAO notes that as of that time, there were 105 HEU-fueled reactors on DOE's list to convert (of which 29 had already fully converted by the time of GAO's report, leaving 76 still using HEU fuel), and 56 more HEU-fueled reactors for which conversion was not planned, for a total of 132 HEU-fueled reactors as of that time. By late 2005, publicly released data from the Global Threat Reduction Initiative (GTRI) program indicated that three more reactors had completed their conversion, bringing the total fully converted to 32, and the total number of reactors targeted for conversion had increased from 105 to 106. See Christopher Landers, "Reactors Identified for Conversion: Reduced Enrichment for Research and Test Reactors (RERTR) Program," in *RERTR 2005: 27th International Meeting on Reduced Enrichment for Research and Test Reactors, Boston, Mass., 6-10 November* (Argonne, Ill.: Argonne National Laboratory, 2005; available at http://www.rertr.anl.gov/RERTR27/PDF/S9-1_Landers.pdf as of 20 June 2006). That meant that as of the end of 2005, there were 74 reactors remaining that were targeted for conversion but were still using some HEU fuel. But there are also other HEU-fueled reactors which were *not* targeted for conversion, some of which were not on the lists provided by DOE to GAO. Data compiled by Frank von Hippel and Alexander Glaser of Princeton University indicates that there are more than 60 operational HEU-fueled research reactors and critical assemblies around the world not covered by the revised target list for conversion, for a total of roughly 135 HEU-fueled research reactors worldwide. (Personal communication from Frank von Hippel, December 2005.) DOE officials report, however, that additional HEU-fueled reactors are still being identified in ongoing visits to facilities, so the total number of HEU-fueled facilities may turn out to be still higher. Interview with DOE officials, December 2005.

[134] U.S. Congress, *DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium.*

[135] Interviews with Argonne National Laboratory and DOE officials, February 2005.

[136] See David Albright and Kimberly Kramer, "Civil HEU Watch: Tracking Inventories of Civil Highly Enriched Uranium," in *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, 2005; available at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html as of 21 July 2005). Albright and Kramer estimate that there are 175 tons of HEU they designate as civilian, including 50 tons in "power and research reactor programs" and 125 tons of U.S. excess HEU (these are rounded figures). But they point out that 15 tons of the U.S. excess is research reactor fuel, and I have therefore included this amount in the total of civilian HEU. I have not included the remainder of the U.S. excess, as Albright and Kramer do, in order to avoid giving an exaggerated impression of the scale of civilian HEU use around the world.

Figure 2.1: Global Military and Civil Stockpiles of Separated Plutonium

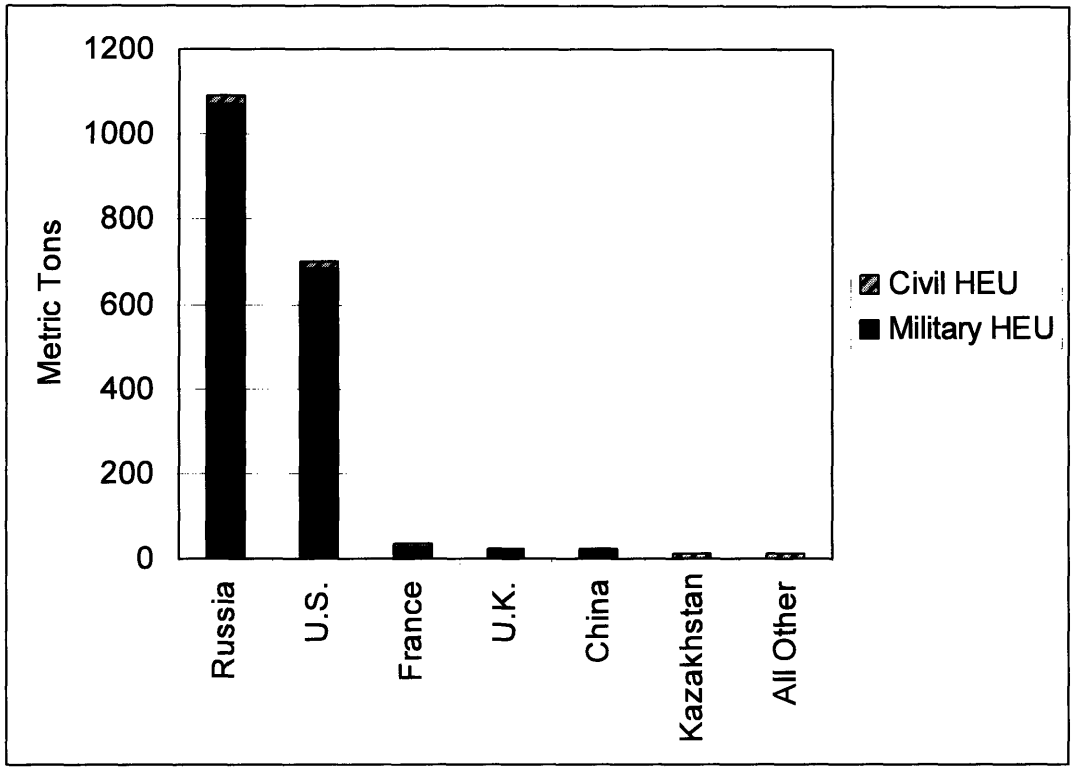


Source: David Albright and Kimberly Kramer, *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, July 2005, available as of 2 January 2007 at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html).

The IAEA does not safeguard military nuclear material, and nuclear weapon states are not required to place their nuclear materials under IAEA safeguards (though a small amount of material in these states, particularly in the United States, is under safeguards under voluntary offer agreements, and French and British civilian material is under Euratom safeguards, integrated with those of the IAEA). Hence, as of the end of 2004 less than 2% of the world's estimated HEU stockpile was under some form of international safeguards (representing 40 tons of HEU, of which 10 tons was excess U.S. HEU), while about and only about 40% of the world's separated plutonium was under international safeguards (representing 200 tons of separated plutonium outside of reactor cores, more than 90% of that in Britain and France).[137]

[137] The separated plutonium under safeguards included 12.4 tons under IAEA safeguards in states with comprehensive or limited safeguards agreements (that is, INFCIRC/153 or INFCIRC/66 agreements); 2 tons of U.S. excess plutonium; 4.4 tons of British excess plutonium; 102.7 tons of civilian plutonium in Britain; and 78.5 tons of civilian plutonium in France. All of the British and French civil plutonium is under Euratom safeguards, and some of it is under IAEA safeguards as well. The HEU under safeguards included 22 tons under IAEA safeguards in countries with comprehensive or limited safeguards agreements; 10 tons of U.S. excess

Figure 2.2: Global Stockpiles of Military and Civil HEU



Source: Albright and Kramer, *Global Stocks of Nuclear Explosive Materials.*

---

material; 6.4 tons of civil HEU in France; and 1.5 tons of civil HEU in the United Kingdom. All of the British and French civil HEU is under Euratom safeguards. For material under comprehensive or limited safeguards agreements, see Table A18 in International Atomic Energy Agency, *Annual Report 2004* (Vienna: IAEA, 2005; available at http://www.iaea.org/Publications/Reports/Anrep2004/anrep2004_full.pdf as of 3 January 2007). For U.S. and British material under safeguards, see Matthew Bunn, "IAEA Monitoring of Excess Nuclear Material," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/monitoring/trilateral.asp as of 23 May 2006). For British and French civil plutonium and HEU, see International Atomic Energy Agency, *Communication Received from the United Kingdom of Great Britain and Northern Ireland Concerning Its Policies Regarding the Management of Plutonium*, INFCIRC/549/Add. 8/8 (Vienna: IAEA, 2006; available at http://www.iaea.org/Publications/Documents/Infcircs/2006/infcirc549a8-8.pdf as of 16 May 2006); International Atomic Energy Agency, *Communication Received from the France Concerning Its Policies Regarding the Management of Plutonium*, INFCIRC/549/Add. 5/9 (Vienna: IAEA, 2005; available at http://www.iaea.org/Publications/Documents/Infcircs/2005/infcirc549a5-9.pdf as of 16 May 2006).For material under comprehensive or limited safeguards agreements, see Table A18 in International Atomic Energy Agency, *Annual Report 2004*. For U.S. and British material under safeguards, see Bunn, "IAEA Monitoring of Excess Nuclear Material." For British and French civil plutonium and HEU, see International Atomic Energy Agency, *Communication Received from the United Kingdom of Great Britain and Northern Ireland Concerning Its Policies Regarding the Management of Plutonium*; International Atomic Energy Agency, *Communication Received from the France Concerning Its*

Because they have both military and civilian uses, these materials are much more broadly distributed than nuclear weapons are. Separated plutonium or HEU exist in hundreds of buildings in more than 40 countries. There are ten countries with two metric tons or more of separated plutonium or HEU, including all of the five NPT nuclear weapon states, India (a non-NPT state), Germany, Japan, Belgium, and Kazakhstan. Thus there are at least three non-nuclear-weapon states under the NPT with enough weapons-usable nuclear material on their soil for hundreds of nuclear weapons.[138] See Table 2.2.

In addition to the countries with tons of weapons-usable nuclear material, there are roughly 26 other countries with "Category I" quantities of weapons-usable nuclear material – that is, enough material that under international standards, the highest levels of security are required (this applies to more than 5 kilograms of U-235 contained in HEU, or more than 2 kilograms of plutonium.)

This includes the three other non-NPT states and 23 additional NPT non-nuclear-weapon states. Of these 26, seven are developing countries and nine are transition countries (that is, former communist countries). Thus, nuclear weapons or enough nuclear material to pose a serious concern exist in a total of some 36 countries. See Table 2.3. Security for these materials in all of these countries must be effective enough to ensure that plausible terrorist and criminal threats, both from insiders and outsiders, can be reliably defeated.

Beyond these countries, quantities of separated plutonium or HEU in the range of roughly one to a few kilograms exist in an additional 13 countries. All of these are NPT non-nuclear weapon states; seven are developing countries, two are transition countries. See Table 2.4. Hence, quantities in the range of a kilogram or more of HEU or separated plutonium exist in roughly 49 countries. Because official information on the stocks of HEU in these different countries is generally not publicly available, these tables are based on partial information and judgment; it may be that a few countries should be added, subtracted, or moved from one table to the other.

Policies Regarding the Management of Plutonium. I am grateful to John Kinney of the IAEA Safeguards Directorate for helping me to clarify this data; personal communication, July 2006.

[138] While Kazakhstan once declared over 10 tons of HEU to the IAEA, the origin of this number is somewhat of a mystery, as Kazakhstan's stocks appear to be much smaller. Nearly three tons of medium-enriched material (in the 20-30% range) existed at Aqtau, the site of the BN-350 fast-neutron reactor, but the fresh fuel for that facility has since been moved to the fuel processing facility at Ust-Kamenogorsk and blended down to LEU. "Government of Kazakhstan and NTI Mark Success of HEU Blend-Down Project: Material Could Have Been Used to Make up to Two Dozen Nuclear Bombs" (Ust-Kamenogorsk, Kazakhstan: Nuclear Threat Initiative, 8 October 2005; available at http://www.nti.org/c_press/release_Kaz_100805.pdf as of 17 December 2005). It is possible that the declaration included the fuel of this type that was already irradiated, which had been HEU when fresh; depending on the burnup, it is likely that this material is now less than 20% enriched and hence no longer HEU. The amount of material remaining at Kazakhstan's HEU-fueled research reactors has not been publicly described, but is in the range of hundreds of kilograms, not several tons.

Table 2.2: Countries With ≥2 Tons of Weapons-Usable Nuclear Material: Stocks Physically Located in Each Country as of the end of 2003, in Metric Tons

Country	Mil. Pu	Civil Pu	Total Pu	Mil. HEU	Civil HEU	Total HEU	Total
Russia	145	38.2	183.2	1070	22.5	1092.5	1276
United States	87	5	92	685	16[a]	701	793
U.K.	3.2	96.3	99.5	21.9	1.546	23.446	123
France	5	78.6	83.6	29	6.382	35.382	119
China	4	0	4	21	1	22	26
Germany	0	11.3	11.3	0	1.04	1.04	12
Japan	0	5.4	5.4	0	1.973	1.973	7
Belgium	0	3.5	3.5	0	0.505	0.505	4
India	0.4	1.25	1.65	0.5	0.0075	0.5075	2
Kazakhstan	0	0[b]	0	0	10.9	10.9	11
All others	0.6	0.15	0.75	1.1	5	6.1	7
Total	245	240	485	1829	67	1895	2380

Sources: Except where otherwise noted, figures are from David Albright and Kimberly Kramer, *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, July 2005, available as of 2 January 2007 at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html). Data for civilian plutonium in Russia, the United States, the United Kingdom, France, Germany, Belgium, Japan, China, and Switzerland and for civil HEU in France, Germany, and the United Kingdom are based on annual official declarations to the IAEA (Information Circular, or INFCIRC, 549). Where ranges were given in the original source, the figures in the table represent the mid-point of the range. Where the data is based on official declarations, all the significant figures in the declarations are included; totals, however, are rounded. Departing from the convention used by Albright and Kramer, plutonium and HEU stockpiles declared excess to military needs are listed in the military columns (reflecting their origin), rather than the civilian columns, to avoid exaggerating the civilian use of these materials. Data for the stocks *owned* by each country would differ: Japan's plutonium figures, for example, would be much higher (as many tons of Japanese separated plutonium are stored in Britain and France), and the figures for Britain and France would each be substantially lower. The "bomb equivalent" estimates are based on 4 kilograms of military plutonium per bomb, 5 kilograms of civilian plutonium per bomb, 15 kilograms of military HEU per bomb, and 30 kilograms of civilian HEU per bomb (reflecting the substantially lower average enrichment level of civilian HEU), except in the case of Kazakhstan; nearly all of the HEU there is known to be of very low enrichment, and hence much larger quantities of it would be needed for a weapon.

[a]Albright and Kramer estimate that 15 tons of the HEU the United States has declared excess is irradiated research reactor fuel and that roughly another 1 ton of HEU is in the cores of U.S. research reactors.

[b]There are three tons of very high-quality plutonium in irradiated breeder blankets from the BN-350 reactor in Kazakhstan. These are not counted here, because they are not separated from the uranium and fission products in the assemblies, but are counted by Albright and Kramer, because much of this material is no longer radioactive enough to meet the IAEA definition of irradiated material and instead counts as unirradiated direct-use material. Hence, the world total estimated in Albright and Kramer is a few tons higher than the world total estimated here.

Table 2.3: Other Countries With Cat. I Quantities of Weapons-Usable Material

Country	NPT-NNWS	Non-NPT	Developing	Developed	Transition
Argentina	Y		Y		
Australia	Y			Y	
Austria	Y			Y	
Belarus	Y				Y
Canada	Y			Y	
Czech Republic	Y				Y
Greece	Y			Y	
Hungary	Y				Y
Israel		Y		Y	
Italy	Y			Y	
Latvia					Y
Libya	Y		Y		
Mexico	Y		Y		
Netherlands	Y			Y	
North Korea		Y	Y		
Pakistan		Y	Y		
Poland	Y				Y
Romania	Y				Y
South Africa	Y		Y		
Spain	Y			Y	
Switzerland	Y			Y	
Taiwan	Y			Y	
Ukraine	Y				Y
Uzbekistan	Y				Y
Vietnam	Y		Y		
Yugoslavia	Y				Y

Sources: Based on data presented in Albright and Kramer, *Global Stocks of Nuclear Explosive Materials.*

The countries with either nuclear weapons or substantial stockpiles of nuclear materials, shown in Tables 2.1 and 2.2, generally have between a dozen and hundreds of buildings where their nuclear stockpiles reside. The countries without nuclear weapons and with between a kilogram and two tons of weapons-usable nuclear material on their soil (shown in Tables 2.3 and 2.4) typically have only one or two buildings with weapons-usable nuclear material, though a small number have up to half a dozen such buildings. No complete estimate of the number of buildings worldwide with a kilogram or more (or a Category I quantity or more) of weapons-usable nuclear material exists; that figure is likely to be over 1,000 buildings (if buildings where nuclear weapons themselves exist are included), but is certainly less than 3,000.

Table 2.4: Other Countries With Kilogram-Range Quantities of Weapons-Usable Material

Country	NPT-NNWS	Non-NPT	Developing	Developed	Transition
Bulgaria	Y				Y
Chile	Y		Y		
Ghana	Y		Y		
Iran	Y		Y		
Jamaica	Y		Y		
Nigeria	Y		Y		
Norway	Y			Y	
Portugal	Y			Y	
Slovenia	Y				Y
South Korea	Y			Y	
Sweden	Y			Y	
Syria	Y		Y		
Turkey	Y		Y		

Source: Based on data presented in Albright and Kramer, *Global Stocks of Nuclear Explosive Materials.*

Transport

Nuclear warheads and weapons-usable materials must be adequately secured not only while they are at fixed facilities, but also while they are being transported – between buildings within sites, between sites, and between countries. Indeed, transport is the stage of these items' life cycle that is most vulnerable to overt, forcible theft, as when these items are being shipped from place to place, it is impossible to provide the multiple layers of detection and delay that can be put in place at a fixed site. This problem is typically addressed with measures such as armed guards accompanying the transports, vehicles with special protection against hijack and sabotage, secrecy concerning the schedule and route of the transports, and continuous or frequent tracking of the transport en route.

The scale and frequency of transport, particularly from site to site within countries, is huge. Hundreds of nuclear warheads are transported from deployment sites to warhead storage and assembly/disassembly facilities, or from such facilities back to deployment sites, each year, in both Russia and the United States – and presumably, to a lesser extent, in other countries with nuclear weapons. In Russia, for example, the U.S. Cooperative Threat Reduction (CTR) program has been planning to pay for roughly 70 shipments per year of nuclear warheads to dismantlement and storage sites, carrying 20-30 warheads each[139] – in addition to however many shipments for operational purposes (which are not paid for by the United States) take place. In the United States, within DOE alone, the Secure Transportation Asset program carries out nearly 100 secure transports of either nuclear warheads or weapons-usable nuclear material a year, at an annual cost that is now in the range of $140 million per

[139] U.S. Department of Defense, *Cooperative Threat Reduction Annual Report to Congress: Fiscal Year 2006* (Washington, D.C.: U.S. Department of Defense, 2005).

year.[140] That does not include Department of Defense transport of nuclear weapons and materials, or private transport of nuclear materials.

Transport of military HEU takes place on a similarly massive scale, as nuclear weapons are dismantled, HEU shipped from dismantlement facilities to HEU storage facilities, and, in both Russia and the United States, excess HEU is shipped to other facilities for blending to LEU. The 30 tons of HEU Russia blends to LEU each year for sale to the United States is shipped from facility to facility and back again over thousands of kilometers of rail, in scores of annual shipments, representing probably the largest annual transport of weapons-usable nuclear material in the world (if measured in ton-kilometers traveled).[141] The scale of shipments of civil HEU is small by comparison, though the hundreds of kilograms of HEU which are shipped each year for fuel for research reactors and as targets for medical isotope production – primarily within the United States and Russia, but also internationally – also pose proliferation risks that must be addressed.[142]

Transport of military plutonium currently occurs at a much smaller scale than transport of military HEU. In the United States, and apparently to a significant degree in Russia as well, plutonium from dismantled weapons is stored at the dismantlement sites, rather than being transported elsewhere for storage, and disposition of excess plutonium – which will lead to this material being transported to processing and fuel fabrication sites and then in the form of fabricated fuel to reactor sites – has not yet gotten underway.

Large quantities of weapons-usable separated plutonium are transported every year in the civil sector, however, as some 20 tons of plutonium is reprocessed from spent fuel and some 10 tons of that is fabricated into fuel for use in nuclear reactors. By one estimate, roughly 100 commercial plutonium shipments occur per year, most of which contain over 100 kilograms of weapons-usable plutonium in a single shipment.[143] In France in particular, which has the world's most active plutonium recycling plutonium, many tons of plutonium separated at the La Hague reprocessing plant each year travel by scores of truck shipments, as

---

[140] In Fiscal Year 2004, for example, the program carried out 91 secure trips carrying nuclear weapons or weapons-usable nuclear material from one place to another – an average of almost two a week. See U.S. Department of Energy, *FY 2006 Congressional Budget Request: National Nuclear Security Administration* (Washington, D.C.: DOE, 2005; available at http://www.cfo.doe.gov/budget/06budget/Content/Volumes/Vol_1_NNSA.pdf as of 18 July 2005), pp. 305-309.

[141] For a simplified map of these shipments, see, for example, U.S. Congress, General Accounting Office, *Status of Transparency Measures for U.S. Purchase of Russian Highly Enriched Uranium* (Washington, D.C.: GAO, 1999; available at http://www.gao.gov/archive/1999/rc99194.pdf as of 18 July 2005), p. 7.

[142] Approximately 800 kilograms of HEU are still used each year by the U.S.-supplied and Russian-supplied reactors currently targeted for conversion to LEU. See Catherine Mendelsohn, "Scope and Accomplishments of the NNSA Nuclear Material Threat Reduction Program," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005). In many cases, however, these shipments are broken up so that individual shipments contain less than a Category I quantity five kilograms of material,U-235 in HEU (designated in the United States and internationally as a "Category I" quantity requiring the highest security standards) in part to avoid the expensive security requirements for Category I material.

[143] David Albright, *Shipments of Weapons-Usable Plutonium in the Commercial Nuclear Industry* (Washington, D.C.: Institute for Science and International Security, 2007; available at http://www.isis-online.org/global_stocks/end2003/plutonium_shipments.pdf as of 3 January 2007).

plutonium oxide, to the fuel fabrication facility at Marcoule; once fabricated into fuel elements, this plutonium is then shipped to numerous reactors both in France and in other countries.[144] Smaller amounts of plutonium oxide are shipped every year to Belgium (which has a smaller MOX fabrication plant) and are shipped from there to other countries for use as fuel. Plutonium separated by reprocessing in Britain is stored at the reprocessing site at Sellafield, without transport, and under current plans much of this plutonium will be fabricated into fuel at the MOX plant at the same site – at which point there will begin to be major shipments of plutonium in fabricated fuel every year from Britain to other countries. Occasionally, substantial shipments of separated plutonium are shipped across the oceans, as when separated plutonium from reprocessing is returned to Japan from France and Britain,[145] or in the recent case when tens of kilograms of weapons plutonium were shipped from the United States to France for fabrication into MOX lead test assemblies for use in a U.S. reactor. The adequacy of security for these transports has been a subject of controversy for many years – and controversies continue.[146]

Rates of Change

Both the size of the global stockpiles of nuclear warheads and weapons-usable nuclear material and their distribution are changing over time – in somewhat different directions.

The total number of nuclear weapons in the world has been declining for over a decade, as the United States and Russia are believed to have dismantled many thousands of nuclear weapons since the 1980s. This decline may be slowing substantially, however. While in some years in the 1990s, the United States dismantled as many as 1800 warheads in a single year, in recent years it appears that this figure has been in the range of 0-300 warheads.[147] The United States has, however, announced a substantial reduction in the planned stockpile of nuclear weapons, which may lead to the dismantlement of some 4,000 weapons by 2012 – though it appears to plan to maintain some 6,000 nuclear warheads indefinitely thereafter.[148] In Russia, some estimates in the 1990s similarly suggested a dismantlement rate in the range of 2,000 a year or even more. But in recent years, Russia has

---

[144] Albright estimates that shipments of plutonium oxide powder from La Hague to Marcoule account for nearly half of total global plutonium shipments. Albright, *Shipments of Weapons-Usable Plutonium*. See also the discussion in Ronald E. Timm, *Security Assessment Report for Plutonium Transport in France* (Paris: Greenpeace International, 2005; available at http://greenpeace.datapps.com/stop-plutonium/en/TimmReportV5.pdf as of 6 December 2005).

[145] These shipments now occur only in the form of fabricated MOX fuel elements.

[146] For a particularly detailed recent analysis of transport security in France, arguing that current procedures are worse than what would be characterized as "high risk" and therefore prohibited within the DOE system, justifying a new category of "extreme risk," see Timm, *Security Assessment Report for Plutonium Transport in France*.

[147] A table of U.S. nuclear warhead dismantlements by year, from 1990-1999, can be found in Robert S. Norris and Hans M. Kristensen, "NRDC Nuclear Notebook: Dismantling U.S. Nuclear Warheads," *Bulletin of the Atomic Scientists* 60, no. 1 (January/February 2004; available at http://www.thebulletin.org/article_nn.php?art_ofn=jf04norris as of 5 December 2005), pp. 72-74.

[148] See, for example, discussion in Robert S. Norris and Hans M. Kristensen, "NRDC Nuclear Notebook: U.S. Nuclear Forces, 2005," *Bulletin of the Atomic Scientists* 61, no. 1 (January/February 2005; available at http://www.thebulletin.org/article_nn.php?art_ofn=jf05norris as of 8 January 2007), pp. 73-75.

closed two of its four weapons assembly and disassembly facilities, suggesting that it now foresees a significantly lower rate of dismantlement in the future (though the two facilities closed had modest capacities compared to the two that remain open).[149] Like the United States, however, it appears that Russia still has some thousands of warheads that are not currently needed either for operational stockpiles or for reserves, which may be dismantled over the next decade.[150] British warhead stockpiles are also declining, and it appears that French stockpiles have been as well. Chinese stockpiles are expected to increase modestly over the next decade, and India, Pakistan, and India are believed to be continuing to produce small numbers of warheads; North Korea may be doing the same, though the fate of its nuclear program will depend in part on the outcome of the six-party talks still underway.

The global distribution of nuclear warheads has also declined somewhat in recent years. With the collapse of the Soviet Union and the 1991-1992 presidential nuclear initiatives, all Soviet nuclear weapons were removed from Eastern Europe, from surface ships, and from the non-Russian states of the former Soviet Union during the the late 1980s and 1990s. Similarly, U.S. nuclear weapons were removed from surface ships and from South Korea in the 1990s. The number of states that possess nuclear weapons of their own (nine) is the same in 2007 as it was 20 years before, as South Africa became the first and only state to completely dismantle a nuclear weapon stockpile that it owned and had full control over – but North Korea, if its declarations of a nuclear weapons capability are correct, has added itself to the list of states with nuclear weapons. Trends over the next 20 years are difficult to predict; it remains possible that the current number of states with nuclear weapons will remain stable or even decline (if international efforts succeed in rolling back North Korea's nuclear program, ensuring that Iran does not develop nuclear weapons, and convincing other states not to follow the nuclear weapons route); but it is also possible that the number of states with nuclear weapons could increase significantly, with both North Korea and Iran becoming full-fledged nuclear powers and a number of other states subsequently choosing to follow the same path.

Like warhead stockpiles, global stockpiles of military HEU have been falling for more than a decade. All of the five NPT nuclear-weapon states have stopped production of HEU for weapons, and the United States and Russia have each declared substantial quantities of military HEU as excess to their military needs. Russia blends 30 tons of excess military HEU each year to LEU for sale to the United States, a program that is expected to continue until 2013, at which point 500 tons of HEU will have been destroyed. Some 285 tons of HEU had been destroyed in this effort by the fall of 2006.[151] Some 82 tons of U.S. excess HEU had

---

[149] See discussion, for example, in Oleg Bukharin, *Russia's Nuclear Complex: Surviving the End of the Cold War* (Princeton, N.J.: Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2004; available at http://www.ransac.org/PDFFrameset.asp?PDF=bukharinminatomsurvivalmay2004.pdf as of 8 March 2005).

[150] Robert S. Norris and Hans M. Kristensen, "NRDC Nuclear Notebook: Russian Nuclear Forces, 2005," *Bulletin of the Atomic Scientists* 61, no. 2 (March/April 2005; available at http://www.thebulletin.org/article_nn.php?art_ofn=ma05norris as of 1 March 2005), pp. 70-72.

[151] USEC, "Chronology: U.S.-Russian Megatons to Megawatts Program: Recycling Nuclear Warheads into Electricity (as of October 1, 2006)" (Bethesda, Md.: USEC, October 2006; available at http://www.usec.com/v2001_02/HTML/Megatons_chronology.asp as of 3 January 2007).

been downblended or shipped for downblending by the end of FY 2005.[152] Pakistan is believed to continue to produce military HEU, though on a small scale compared to the destruction of HEU in the United States and Russia; India is thought also to have modest military HEU production underway, though plutonium is the primary focus of its military nuclear material production program. North Korea is reported to be endeavoring to establish a military HEU production capability, but U.S. intelligence assesses that it is still some years away from acquiring such a capability. Iran is working to establish a large-scale enrichment facility which it insists is for solely peaceful purposes; others are concerned that this facility or others established covertly might be turned to military purposes. Civil HEU stockpiles have been growing modestly, as the pace at which research reactors discharge irradiated HEU and load more has been greater than the pace at which this HEU has been blended or disposed of, but these stockpiles remain tiny by comparison to military stockpiles.

Global military plutonium stockpiles are nearly static. All of the five NPT nuclear-weapon states have stopped producing plutonium for use in weapons weapons – though in Russia, three plutonium production reactors continue to operate, churning out some 1.2 tons of plutonium a year, because they also provide essential heat and power for nearby Siberian communities. India, Israel, and North Korea are believed to continue small-scale production of military plutonium, and such production has recently begun in Pakistan as well, complementing Pakistan's primary focus on HEU. As noted above, disposition of excess military plutonium has not yet gotten underway. Civil plutonium stockpiles continue to increase dramatically. Every year, nuclear power plants around the world discharge some 8,000 tons of spent fuel, containing some 80 tons of plutonium. Roughly one-quarter of this fuel is reprocessed each year, yielding some 20 tons of separated plutonium. Only about half of that plutonium separated by reprocessing is fabricated into fuel each year, with the remainder remaining in storage. Hence, the global stockpile of separated civilian plutonium increases by roughly 10 tons each year.

The global distribution of separated plutonium and HEU is changing only slowly. All of the countries with substantial stockpiles, shown in Table 2.2, have had stockpiles for decades. Essentially all of the countries with smaller stockpiles, on Tables 2.3 and 2.4, have had at least modest stockpiles of weapons-usable nuclear material for decades. With respect to HEU, the trend is toward fewer and fewer countries having stockpiles, as the U.S. and Russian efforts to convince countries to send back the HEU they exported gain momentum. With respect to separated plutonium, the global distribution is likely to be static or nearly so for some time to come, as few additional countries are interested in pursuing a plutonium fuel cycle, but those who have separated plutonium on their soil are finding it hard to get rid of (though Belgium is one example of a country that has burned all or nearly all of the separated plutonium it owned as MOX fuel).[153]

---

[152] U.S. Department of Energy, *FY 2007 Congressional Budget Request: National Nuclear Security Administration--Defense Nuclear Nonproliferation*, vol. 1, DOE/CF-002 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_1_NNSA.pdf as of 3 January 2007), p. 535.

[153] See, for example, Albright, *Shipments of Weapons-Usable Plutonium*.

Widely Varying Nuclear Security

Those seeking material for a nuclear bomb will go wherever it is easiest to steal, or buy it from anyone willing to sell. Thus, security for bomb material is only as good as its weakest link. Insecure nuclear bomb material anywhere is a threat to everyone, everywhere. Yet today, there are no binding international standards for how well nuclear weapons and materials should be secured. Nuclear security levels are left to the discretion of each of the dozens of states that possess such stockpiles, with the result that security for stocks of potential nuclear weapons materials varies enormously, from excellent to appalling.

It is important to understand that the nuclear Nonproliferation Treaty (NPT) does not contain any provisions requiring states to secure nuclear material from theft.[154] Similarly, the IAEA safeguards system is designed only to verify that states have not diverted nuclear material for nuclear explosives, not to protect material from theft or even to confirm that the state that owns the material is providing adequate protection.[155] Indeed, because of the long times between inspections at many sites, the IAEA would not typically be able to detect that a theft had occurred until days, weeks, or months after the fact. In any case, some 90% of the world's separated plutonium and HEU is *not* under either IAEA or Euratom safeguards.

There is an international Convention on Physical Protection of Nuclear Materials, but it currently applies only to material in international transport, not to the more than 99% of the world's nuclear material that is in domestic storage, use, or transport within individual countries. Even when the recently approved amendment to cover domestic material enters into force (expected to take years), the convention will still exclude all military nuclear material (nearly 90% of the total world stockpile of weapons-usable nuclear material). Moreover, the amendment will not create any binding global nuclear security standards with enough specifics to be effective – though it does offer a number of generally worded principles that should help in convincing states to strengthen nuclear security. For example, the amended convention will require parties to have a domestic rule concerning how much security facilities with nuclear material must provide, but it will not impose any substantial requirements concerning what that rule should say.[156]

---

[154] One of the treaty's negotiators has emphasized that if he knew then what he knows now, he would have sought to include such provisions. See remarks by George Bunn at International Atomic Energy Agency, *Proceedings of the Symposium on International Safeguards: Verification and Nuclear Material Security, Vienna, 29 October-2 November 2001* (Vienna: IAEA, 2001).

[155] Non-nuclear-weapon states subject to full-scope IAEA safeguards are required to make comprehensive reports on their nuclear inventories and changes in them to the IAEA, and this imposes an international discipline that tends to improve the quality of nuclear material accounting, which is one element in an overall nuclear security system.

[156] For the text of the current convention, see International Atomic Energy Agency, *The Convention on Physical Protection of Nuclear Material*, INFCIRC/274/Rev. 1 (Vienna: IAEA, 1980; available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml as of 29 July 2005). For the text of the approved amendment, see *Amendment to the Convention on the Physical Protection of Nuclear Material* (Vienna: International Atomic Energy Agency, 2005; available at http://www-pub.iaea.org/MTCD/Meetings/ccpnmdocs/cppnm_proposal.pdf as of 16 September 2005). The convention and the amendment negotiations are described in detail in Chapter 5.

The IAEA publishes recommendations on physical protection for nuclear materials and facilities which are somewhat more specific, but these are purely advisory and are still quite general – it is quite possible to comply fully with these recommendations and not have a secure system.[157] Because of disagreements among some of the states participating in the development of the recommendations, for example, following the IAEA recommendations does not necessarily require having *any* armed guards at a site with plutonium or HEU, and the recommendations do not specify any particular threat that facilities should be able to defeat.

A number of major nuclear suppliers, including the United States, have adopted policies or laws that require countries they supply to meet some requirements for physical protection for the supplied nuclear material. The United States, in particular, is required by law to ensure that recipient countries meet adequate physical protection standards and has nuclear supply agreements under which it has provided HEU to scores of countries around the world. Its nuclear supply agreements with foreign countries typically require that the recipient country provide "levels of physical protection" for the supplied nuclear material "at least equivalent" to those in the IAEA recommendations.[158] The Nuclear Suppliers' Group (NSG), a cartel of the major nuclear suppliers, has agreed that all of its participants will require that recipients of major nuclear exports meet at least a more general set of physical protection criteria; these refer to the IAEA recommendations, but only as a "useful basis for guiding" recipient states in designing their physical protection systems, not as a requirement.[159] Similarly, a number of states have entered into agreements in other contexts that require certain levels of physical protection – in some cases to implement the IAEA recommendations. These include the U.S.-Russian Highly Enriched Uranium Purchase Agreement and in the African Nuclear Weapon Free Zone.[160]

Information on the specific measures taken to secure nuclear stockpiles around the world is typically secret, to keep potential terrorists and thieves from guessing what security measures they may be up against at a particular site. Hence it is effectively impossible, in an unclassified publication, to put together a complete picture of security for nuclear weapons and materials around the world. As far as is publicly known, no one – not the U.S.

---

[157] For the text of the IAEA recommendations, see International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected) (Vienna: IAEA, 1999; available at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html as of 22 December 2006). The development of these recommendations is described in Chapter 5.

[158] *Agreement for Co-Operation between the Government of the United States of America and the Swiss Federal Council Concerning Peaceful Uses of Nuclear Energy* (Washington, D.C.: U.S. Department of Energy, 1997; available at http://www.nnsa.doe.gov/na-20/docs/Switzerland_Agam.pdf as of 19 July 2005).

[159] The NSG Guidelines are contained in International Atomic Energy Agency, *Communications Received from Certain Member States Regarding Guidelines for the Export of Nuclear Material, Equipment and Technology*, INFCIRC/254/Rev. 7/Part 1 (Vienna: IAEA, 2005; available at http://www.nuclearsuppliersgroup.org/PDF/infcirc254r7p1-050223.pdf as of 20 July 2005). The physical protection discussion is in paragraph 3 of the guidelines and Annex C.

[160] See discussion in Bonnie Jenkins, "Establishing International Standards for Physical Protection of Nuclear Material," *Nonproliferation Review* 5, no. 3 (Spring-Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/jenkin53.pdf as of 19 July 2005).

government, not the International Atomic Energy Agency, not any other government or organization, as far as is known – has such a complete picture today: while a great deal is known about the risks at some particular sites, no one knows for sure which sites, judged on a global basis, pose the highest risks and should be the highest priorities for policy steps to reduce the risks.[161]

Nevertheless, from the unclassified information that is available, it is clear that security arrangements vary widely from one country and facility to another,[162] and in a troubling number of cases would likely not be sufficient to deal with either a well-planned insider theft or an attack by a significant number of well-armed and well-trained outsiders. Until the 9/11 attacks, for example, several countries did not require *any* armed guards at nuclear facilities – including Japan, which has tons of weapons-usable separated plutonium and hundreds of kilograms of HEU metal on its soil, enough material for many hundreds of nuclear weapons and was the nation where the Aum Shinrikyo terror cult was working actively to get nuclear weapons and the materials to make them.[163] (Since the 9/11 attacks, Japan has posted armed units of its national police to guard nuclear facilities – but these are apparently not fully integrated with the security plans at the sites, and many of them patrol at the perimeters, where they look impressive but would be vulnerable to being shot in the opening moments of an attack.[164])

---

[161] While the defense authorization for Fiscal Year 2005 required DOE to prepare a prioritized list of the highest-risk sites worldwide and a plan for addressing them, DOE provided three separate lists corresponding to the priorities of three different programs, none of which were based on realistic assessments combining the quality and quantity of material at particular sites with the security at those sites and the threats those sites faced. Xxx get ref for actual list For discussion of such an approach, see Chapter 4.

[162] See, for example, discussion in George Bunn and Lyudmila Zaitseva, "Guarding Nuclear Reactors and Materials from Terrorists and Thieves," in *IAEA Symposium on International Safeguards: Verification & Nuclear Material Security* (Vienna: International Atomic Energy Agency, 2001; available at http://www.iaea.org/worldatom/Meetings/2001/infsm367progr_fr.shtml as of 13 June 2006).

[163] These countries relied instead on detection and barrier technologies to provide warning and delay any theft until off-site police forces could arrive. Tests in the United States suggest that such an approach would be likely to fail in the face of well-equipped and well-trained attackers, because of the remarkable speed with which various barriers can be breached. The reluctance to have armed units at nuclear sites reflected a Japanese culture in which possession of firearms by private citizens has been forbidden for centuries and where even policemen are usually not armed. (Britain, which has a similar tradition of tight constraints on the kinds of armament that private guards may have, and of unarmed policemen, set up a separate force – the Atomic Energy Constabulary – to guard nuclear facilities.) For a discussion of the Japanese view on this matter pre-9/11, confirming that "the guards do not carry firearms on duty at any nuclear facility in Japan" (as of 1997), see Hiroyoshi Kurihara, "The Protection of Fissile Materials in Japan," in *A Comparative Analysis of Approaches to the Protection of Fissile Materials: Proceedings of the Workshop at Stanford University, July 28-30, 1997* (Livermore, Cal.: Lawrence Livermore National Laboratory, 1997). Similarly, in Canada, which has more than a ton of HEU on its soil, the pre-9/11 rules only required enough guards on-site to perform tasks such as checking identification and manning monitors; armed response to possible attack was to rely on forces arriving from off-site. See Government of Canada, "Nuclear Safety and Control Act: Nuclear Security Regulations," *Canada Gazette Part II* 134, no. 13 (21 June 2000; available at http://canadagazette.gc.ca/partII/2000/20000621/pdf/g2-13413.pdf as of 20 November 2006). Nuclear security measures in both Canada and Japan are discussed in more detail in Chapter 4. A number of other countries also do not require armed guards at nuclear facilities.

[164] Interviews with Japanese experts and U.S. experts, and author's observations during a visit to a Category I facility in Japan, November 2006. See also, Tatsujiro Suzuki, "Implications of 09/11 Terrorism for Civilian

Many countries have not defined in regulations or other rules any particular threat that nuclear security systems have to be able to defeat (known as the "design basis threat," or DBT, because it is the threat that is the basis for designing the security system); they have relied instead on setting rules regarding how high fences should be, what types of locks and vaults should be provided, and the like. Many experts believe that having rules requiring a particular level of performance from the security system, rather than a compliance-based approach where rules simply require that particular technologies and procedures be in place, is crucial to good security. As one U.S. expert put it, "if you don't have a DBT, you don't have good security."[165] As of the end of 2006, this category of countries with no regulatory DBT in place still included Russia, among many others, although a new rule including a DBT is expected soon.[166]

A review of presentations about their approaches to physical protection made by 19 countries at conferences in the late 1990s noted wide variations in their nuclear security approaches and practices. For example, 12 of the 19 reported that they perceived a threat of insider theft and took measures to address that problem, six provided no information at all on the insider problem, and one country insisted that it faced no threat from insiders. Only 11 of the 19 reported that they required facilities to protect against sabotage, as well as against theft of nuclear material.[167] In responses to a detailed survey on nuclear security practices prepared by researchers at Stanford University, five of the six respondents said they had a DBT in place, but two of the six said they did not take into account any risk of an attack by terrorists in their DBT; three of the six said their DBT did not include dangers from insiders (either for theft or for sabotage); none of the six reported having made any provision to deal with the threat of sabotage by a large truck bomb set off beyond the protected area; two of the six did not require armed guards to protect areas with weapons-usable nuclear material; most required that when operations were done in an area with weapons-usable nuclear material at least two persons had to be present ("two-man rule"), but "that requirement was administered in quite different ways and in some cases not followed."[168]

Nuclear Industry and its Response Strategy," presentation to the Japan Atomic Industrial Forum-Harvard University Nonproliferation Workshop, January 30-31, 2002. Security at nuclear facilities in Japan and Canada, among several other countries, is discussed in more detail in Chapter 4.

[165] Byron Gardner, Sandia National Laboratories, personal communication, March 1995.

[166] Russian officials have been projecting that a substantially modified version of the basic rules of physical protection would be issued imminently since at least the spring of 2005; this regulation would include a requirement for facilities to meet a particular DBTdesign-basis threat (the details of which would be specified in a separate, classified document). Interviews with Boris Kroupchatnikov, Rostekhnadzor, May 2005 and October 2005. (Kroupchatnikov is in overall charge of regulating physical protection and material control and accounting for all nuclear materials in Russia outside the Ministry of Defense and the portions of Rosatom involved in manufacturing nuclear weapons and components.) As of late 2006, however, the regulation had not yet been issued.

[167] Kevin J. Harrington, *Physical Protection of Nuclear Material: National Comparisons* (Livermore, Cal.: Sandia National Laboratories in cooperation with Stanford University, Center for International Security and Cooperation, 1999).

[168] The most detailed publicly available discussion of the results of this survey is in Bunn and Zaitseva, "Guarding Nuclear Reactors and Materials from Terrorists and Thieves."

Too little data is publicly available to provide a detailed country-by-country review of nuclear security arrangements in each of the countries in Tables 2.1-2.4, which would in any case be beyond the scope of this chapter. A review of the information that is publicly available concerning security levels at different sites in different countries, quantities and qualities of material at those sites, and the threats that security systems in different countries must face suggests that as of 2005, the most urgent risks of nuclear theft existed in Russia; at research reactors fueled with HEU around the world; and in Pakistan. Each of these particularly high-priority examples are discussed in turn below.

Nuclear Security in Russia – Yesterday and Today

The breakup of the Soviet Union in 1991 created a danger unprecedented in human history – the collapse of an empire armed with tens of thousands of nuclear weapons and enough nuclear material for tens of thousands more. The world has been extraordinarily lucky that this collapse involved so little violence and that a horrifying outpouring of weapons of mass destruction and related materials and technologies did not occur. Substantial progress has been made in the years since the Soviet collapse, and Russia today is a very different country than Russia in the mid-1990s. But crucial risks remain, and urgent action is needed to address them.

The Soviet Union had a highly effective and intelligently designed security system for its nuclear weapons and nuclear materials – but it was designed for a world that no longer exists. A security system designed for a single state with a closed society, closed borders, and well-paid, well-cared-for nuclear workers was splintered among multiple states with open societies, open borders, desperate, underpaid nuclear workers, and rampant theft and corruption – a situation the system was never designed to address.[169] Given the tightly controlled nature of Soviet society, there had been no expectation that there would be terrorist teams operating on Soviet territory, and therefore the need to protect against armed outside attack on nuclear facilities in peacetime had been modest.

Similarly, little investment had been made in Soviet times in technical systems to protect against insider theft threats, as nuclear insiders were carefully screened, well compensated, and closely watched: if they did steal something, they could not meet with a foreigner or leave the country in an attempt to sell it without being very closely monitored by

---

[169] For summaries of the nuclear security situation in the former Soviet Union in the years following the Soviet collapse, see, for example, John Deutch, then Director of Central Intelligence, "The Threat of Nuclear Diversion," in *Global Proliferation of Weapons of Mass Destruction, Part II*; Matthew Bunn, *The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material* (Washington, D.C.: Managing the Atom Project, Harvard University, and Non-Proliferation Project, Carnegie Endowment for International Peace, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/FullNextWave.pdf as of 2 January 2007); Oleg Bukharin, "Security of Fissile Materials in Russia," *Annual Review of Energy and the Environment* 21 (1996); Frank von Hippel, "Fissile Material Security in the Post-Cold War World," *Physics Today* 48, no. 6 (June 1995); Graham T. Allison et al., *Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nulcear Weapons and Fissile Material* (Cambridge, MA: MIT Press, 1996); Oleg Bukharin and William Potter, "Potatoes Were Guarded Better," *Bulletin of the Atomic Scientists* 51, no. 3 (May-June 1995), pp. 46-50; "'We Cannot Preclude the Possibility of Nuclear Materials Theft' (Edited Transcript of Duma Hearing)," *Yaderny Kontrol Digest* 5 (Fall 1997).

the KGB. For these reasons, when the Soviet Union collapsed, most nuclear facilities did not have any detector at the door that would set off an alarm if plutonium or HEU were being carried out (known as "portal monitors"); most did not have security cameras in the areas where the plutonium and HEU were stored and handled; there was an accounting system intended primarily to monitor facilities' performance in meeting their production quotas, never intended to be able to detect nuclear material thefts; the padlocks on doors into nuclear material areas were often of types that could be cut in seconds using a bolt-cutter from any hardware store; and wax seals – the same technology Louis XIV used to seal his letters – were still in wide use to indicate whether containers had been tampered with or vaults opened (allowing any worker with an authorized stamp to break the seal, remove material, and replace the seal with an identical one without detection).

Moreover, funding to maintain nuclear security systems plunged in the years following the Soviet collapse, leading to gaping holes in security fences, alarm systems that no longer worked, and the like – situations that in several cases were, in fact, exploited by individuals who stole HEU or separated plutonium. In one case in which a naval officer walked through a giant hole in the fence at a naval base, snapped the padlock on a shed, put several kilograms of HEU in his backpack, and walked off without detection, the military prosecutor concluded that "potatoes were guarded better."[170] Even then-Russian Minister of Atomic Energy Evgeniy Adamov acknowledged in 1998 that "the weakening of our ability to manage nuclear material has been immeasurable."[171] In 1996, the U.S. Director of Central Intelligence testified that weapons-usable nuclear materials "are more accessible now than at any other time in history – due primarily to the dissolution of the former Soviet Union and the region's worsening economic conditions," and that *none* of the facilities handling plutonium or HEU in the former Soviet states had "adequate safeguards or security measures" in place.[172]

Figure 2.3 shows Building 116 at the Kurchatov Institute in Moscow in 1994, before cooperative U.S.-Russian efforts to upgrade security there began. More than enough HEU for a bomb was present in this building – an example of the conditions of nuclear security in the years following the Soviet collapse. There is, in fact, a fence in the photograph, though it is so overgrown with weeds that it is difficult to make out. (Extensive security upgrades have since been installed for Building 116 and for the other buildings at the Kurchatov Institute containing weapons-usable material.) Figure 2.4 shows a typical easily-cut padlock securing a room containing nuclear material during this period, along with a typical easily-faked seal from this period. (Seals of similar types are still in wide use.)

---

[170] Bukharin and Potter, "Potatoes Were Guarded Better."
[171] Quoted in Nick Wadhams, "Center to Track Russian Nuclear Material," *Associated Press*, 4 November 1998.
[172] Deutch, testimony in *Global Proliferation of Weapons of Mass Destruction, Part II.*

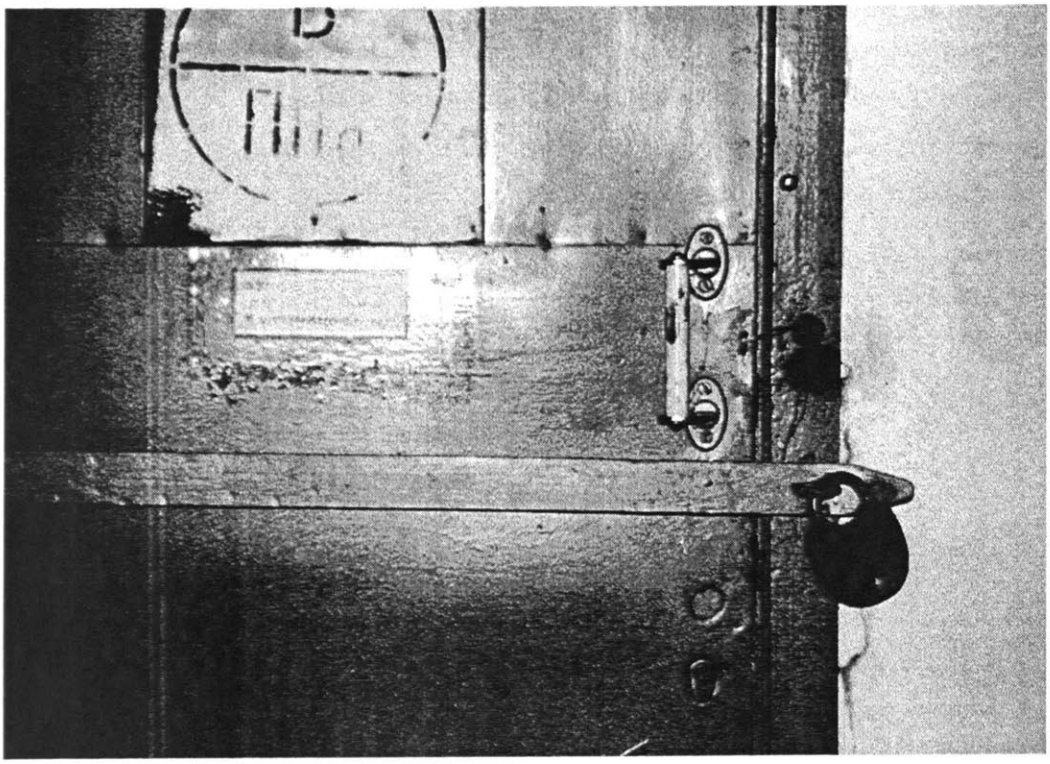
Figure 2.3: Moscow Building With Enough HEU for a Bomb, 1994

Source: DOE

Nuclear security in Russia (where all the Soviet Union's nuclear weapons and more than 99% of its weapons-usable nuclear materials, now resides) has improved substantially in the years since the Soviet collapse. Russia and the states of the former Soviet Union deserve considerable credit for preventing the massive nuclear leakage that many feared in the years immediately following the Soviet Union's collapse – taking action in many cases under very difficult circumstances. Some senior Russian officials have recently claimed that all stockpiles of nuclear weapons and weapons-usable materials are now secure: in April 2004, for example, Minister of Defense Sergei Ivanov said that he could say "with full responsibility" that "no leakage of such materials is possible."[173] Unfortunately, Ivanov's optimistic conclusion cannot be sustained. While security for nuclear stockpiles in Russia continues to improve, security in many cases still falls far short of what is needed to be able to defeat the outsider and insider threats terrorists and criminals have shown they can pose.

[173] Sergei Ivanov, "Remarks to the Center for Defense Information" (Washington, D.C.: CDI, 6 April 2004).

Figure 2.4: Ineffective Seal and Easily-Cut Padlock on Nuclear Material Door



Source: DOE

Indeed, recent anecdotal evidence, described below, suggests that the "demand side" of nuclear smuggling is coalescing more than had been observed before.

The biggest improvements in nuclear security are the result of Russia's stabilization. Russia in 2005 is a very different country from Russia in 1992, or even Russia in 1998. The economy has been growing steadily for several years, the Russian government has stabilized, the federal budget has shifted from huge deficits to noticeable surpluses, and the government has asserted stronger control over key sectors and facilities. As a result, nuclear workers are getting paid a reasonable wage, on time, reducing the danger that desperation might motivate someone to steal nuclear material or sell nuclear secrets. Nuclear facility guards are no longer leaving their posts to forage for food (though pay for nuclear guards apparently remains low). No longer are alarm systems shutting down because the facility failed to pay its electric bill.

In addition, with funds from the United States, Russia's own budget, and limited support from other countries, substantial improvements have been made in security and accounting for nuclear materials and nuclear warheads at many sites. By the end of fiscal year (FY) 2004, U.S.-funded comprehensive security and accounting upgrades had been completed at 75% of the sites with weapons-usable nuclear material in Russia (along with all

of the sites with such material in the non-Russian states of the former Soviet Union).[174] While such comprehensive upgrades had been completed for 75% of the *sites,* however, they had been completed for only 25% of the potentially vulnerable nuclear *material,* as vast quantities of material are believed to be located at a small number of large nuclear defense complex sites, where progress has been slowed by disputes over how much access U.S. experts will receive in the course of implementing U.S.-funded security upgrades.[175]

Several rounds of Russian-funded security upgrades have been undertaken at the direction of the Russian government, in response to terrorist incidents from 1999 to the present. Russian officials report that these have included: increased protective forces at some nuclear facilities; enlarged areas around facilities where access is restricted; an increase in the frequency of training and exercises simulating possible terrorist attacks; and investments in portal monitors, intrusion detectors, security cameras, and the like at individual sites.[176]

By these means, the most egregious weaknesses of the 1990s have largely been addressed. The systems now in place would likely protect reasonably well against casual, poorly planned theft by a single insider or a single outsider – which appears to have been the dominant type of theft that occurred in the known cases from the 1990s. Nevertheless, a variety of indicators suggest that serious weaknesses remain:

- Russian government funding for nuclear security remains far below what is needed. In May 2005, one knowledgeable Russian expert publicly estimated that funding for physical

---

[174] Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 2 January 2007), pp. 30-37.

[175] As these facilities are located in fenced-in, guarded cities, with an additional fence and guard force for the nuclear facility itself, the danger of overt, armed outsider attack is probably less at these facilities than the danger of insider theft. A number of incidents, however, have confirmed that at some of these sites there are well-worn paths through holes in the fence around the city and in some cases holes in the fence around the nuclear facility itself as well.

[176] See, for example, Yuri Volodin, Boris Kroupchatnikov, and Alexander Sanin, "MPC&A Regulatory Program in the Russian Federation: Trends and Prospective," in *Proceedings of the 43rd Annual Meeting of the Institute of Nuclear Materials Management, Orlando, Fla., 23-27 June 2002* (Northbrook, Ill.: INMM, 2002); Dmitry Kovchegin, "Approaches to Design Basis Threat in Russia in the Context of Significant Increase of Terrorist Activity," in *Proceedings of the 44th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 13-17 July 2003* (Northbrook, Ill.: INMM, 2003; available at http://bcsia.ksg.harvard.edu/publication.cfm?program=STPP&ctype=paper&item_id=398 as of 22 March 2005). Russia sent additional troops to defend nuclear sites as the Beslan crisis was unfolding. See Christina Applegarth, "Russia, U.S. Bolster Regional Nuclear Security Following Terrorist Attacks," *Arms Control Today* (October 2004; available at http://www.armscontrol.org/act/2004_10/GTRI.asp as of 5 April 2006). In early 2005, the Russian government approved a new plan for safety and security, but most of the plan involved preparations to take new measures, rather than implementing major new steps immediately. See *Plan Meropriyatii, Cvyazannykh S Vypolneniem Pervogo Etapa Pealizatsii 'Osnov Gosudarstvennoi Politiki V Oblast'i Obespecheniya Yadernoi I Radiatsionnoi Bezopasnost'i Rossiskoi Federatsii Na Period Do 2010 Goda I Dal'neishuyu Perspektivu' (Action Plan for Phase One of the Implementation of 'Foundations of Government Policy in the Area of Nuclear Safety and Radiation Protection within the Russian Federation for the Period to 2010 and Beyond')*, trans. U.S. Department of Energy, Order No. 117-r (Moscow: Government of the Russian Federation, 2005; available at http://www.government.ru/data/news_text.html?he_id=103&news_id=16586 as of 25 February 2005).

protection covers only 30% of the need.[177] In March 2003 testimony to the Russian Duma, then-Minister of Atomic Energy Alexander Rumiantsev warned that $450 million was needed over the next six years to bolster security at Russia's nuclear facilities, that guard forces at nuclear facilities had been cut back due to budget constraints, and that 4–5 times current spending was needed to secure Russian nuclear power plants from sabotage. "Everything boils down to money," he said. At the same hearing, Yuri Vishnevsky, then chairman of Russia's nuclear regulatory agency, said that the government program to ensure nuclear and radiological safety and security received only 10–15% of the funds it required each year.[178] In mid-2005, a representative of one major Rosatom nuclear facility estimated that 90% or more of all funds spent for purchasing or maintaining physical protection, material control, and material accounting equipment at that site came from U.S. money, rather than Russian funds, and described a difficult months-long (and often unsuccessful) process for requesting Russian funds for security upgrades.[179]

- Experts who visit Russia's nuclear facilities continue to report problems such as dilapidated fences, antiquated or broken intrusion detectors, ineffective tamper-indicating devices, undermanned guard forces without night-vision goggles or hardened fighting positions, material accounting systems that would not be able to detect that material had been removed in a timely manner, and the like.[180] In March 2005, the commander of the Ministry of Interior (MVD) troops for the Moscow district said that only seven of the critical guarded facilities in the district had adequately maintained security equipment, while 39 had "serious shortcomings" in their physical protection.[181]
- In general, at each new facility where Russia grants access to U.S. personnel and cooperative work begins, U.S. and Russian experts rapidly agree that a wide range of security and accounting upgrades are needed.
- In 2003, the chief of security at Seversk, Russia's largest plutonium and HEU processing facility, reported that the Ministry of Interior troops guarding the facility routinely failed to protect the facility from outside attack in tests; routinely failed to prevent insiders from removing material in tests; often patrolled with no ammunition in their guns; and were frequently corrupt, becoming "the most dangerous internal violators."[182]
- Both Russian and American experts have reported a systemic problem of inadequate security culture at many sites – intrusion detectors turned off when the guards get annoyed

---

[177] Nikolai N. Shemigon, director-general, Eleron (Rosatom's physical protection firm), remarks to Institute of Physics and Power Engineering, "Third Russian International Conference on Nuclear Material Protection, Control, and Accounting," Obninsk, Russia, 16-20 May 2005.

[178] Robert Serebrennikov, "2002 Saw Several Thefts of Nuclear Materials, Isotope Products in Russia," *ITAR-TASS*, 5 March 2003.

[179] Interview with expert from Russian nuclear facility, July 2005.

[180] Interviews with U.S. laboratory personnel, 2002–2004.

[181] See "Over 4,000 Trespassers Detained at Moscow District Restricted Access Facilities," *Interfax-Agentstvo Voyennykh Novostey*, 18 March 2005.

[182] Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii (Reforming MVD Troops to Guard Russian Nuclear Facilities)," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9, no. 4 (Winter 2003; available at http://www.pircenter.org/data/publications/yk4-2003.pdf as of 28 February 2005).

by their false alarms, doors left open, senior managers allowed to bypass security systems, effective procedures for operating the new security and accounting systems either not written or not followed, and the like.[183] The Seversk security chief's report of guards patrolling without ammunition – and with little understanding of the importance of what they were guarding – is one particularly troubling example.

As a CIA report summed it up in November 2004: "Russia's nuclear security has been slowly improving over the last several years, but risks remain."[184] Even Alexander Rumiantsev, head of Russia's Federal Agency for Atomic Energy (Rosatom, formerly Minatom), warned after the September 2004 terrorist attacks in Russia that "today, we have to admit that we cannot fully rule out the possibility that fissile materials, including highly-enriched uranium and plutonium, as well as technologies suitable for manufacturing nuclear weapons, may fall into the hands of international terrorists."[185]

The outsider and insider threats that nuclear security systems in Russia face are frighteningly high. Russia is the only country in the world where senior officials have confirmed that terrorist teams have actually carried out reconnaissance at nuclear weapon storage facilities. As noted above, senior Russian officials and the Russian state newspaper have reported four incidents in 2001-2002 of terrorist teams carrying out reconnaissance on Russian nuclear warheads – two on nuclear weapon storage facilities and two on nuclear weapon transport trains.[186] The locations of these facilities and the routes of these trains are state secrets in Russia – but secrets the terrorists apparently managed to penetrate.

Few nuclear facilities in Russia (or elsewhere, for that matter) could defend against an attack on the scale of the Beslan school massacre in Russia in September 2004 – 32 suicidal terrorists, armed with machine guns, rocket-propelled grenades, and explosives, launching a

---

[183] Indeed, on one visit to a facility whose security had been upgraded with U.S. assistance, the U.S. General Accounting Office found that the gate to the central storage facility for the site's nuclear material was left wide open and unattended. At another site, guards did not respond when visitors entering the site set off the metal detectors, and the portal monitors to detect removal of nuclear material were not working. See U.S. Congress, General Accounting Office, *Nuclear Nonproliferation: Security of Russia's Nuclear Material Improving; Further Enhancements Needed*, GAO-01-312 (Washington, D.C.: GAO, 2001; available at http://www.gao.gov/new.items/d01312.pdf as of 2 January 2007), pp. 12-13. For a useful discussion of the security culture problem generally, see Igor Khripunov and James Holmes, eds., *Nuclear Security Culture: The Case of Russia* (Athens, Georgia: Center for International Trade and Security, The University of Georgia, 2004; available at http://www.uga.edu/cits/documents/pdf/Security%20Culture%20Report%2020041118.pdf as of 18 February 2005). See also Irina Kupriyanova, "Assessing the Effectiveness of the U.S. Nuclear Material Accounting, Control, and Physical Protection Program in Russia," *Yaderny Kontrol* 7, no. 2 (March/April 2002).

[184] U.S. National Intelligence Council, *Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces* (Washington, D.C.: Central Intelligence Agency, 2004; available at http://www.dni.gov/nic/special_russiannuke04.html as of 5 March 2005).

[185] "Top Russian Official Does Not Rule out International Terrorists May Obtain Nuclear Materials," *Interfax News Service*, 18 September 2004.

[186] Original reporting of the incidents of reconnaissance on warhead transport trains is in Bogdanov, "A Pass to Warheads Found on a Terrorist." General Igor Valynkin, the commander of the force that guards Russia's nuclear weapons, confirmed these reports in "Russia: Terror Groups Scoped Nuke Site." These incidents are also referred to in U.S. National Intelligence Council, *Safety and Security of Russian Nuclear Facilities and Military Forces*.

carefully planned attack with no warning. Nor is that size of attack the upper limit: the Beslan attackers had acquired some of their weapons stockpile in a June 2004 raid on Russian Interior Ministry buildings and arms depots in the neighboring province of Ingushetia that involved at least 200 attackers and left some 80 people dead. In that raid, the attackers, dressed in uniforms of the Russian Federal Security Service, Army intelligence, and other special police squads, overwhelmed local forces, who did not receive reinforcements from federal security service troops for several hours.[187] (This is particularly distressing since the usual approach to security at nuclear facilities – including nuclear weapon storage sites – is to have a relatively modest defensive force on-site and to rely on reinforcements arriving in a timely way.)

Such problems extend beyond Russia's southern borderlands. Attackers have shown repeatedly that they can mass forces seemingly anywhere in Russia without warning and that they can bribe or otherwise collude with insiders. In the week before the Beslan attack, suicide bombers paid bribes and eluded lax airport security to get on two flights out of Moscow, killing all 90 passengers aboard.[188] In October 2004, a month after the Beslan attack, a force of 47 men identified as Dagestanis, armed with clubs and crowbars, seized complete control of a secret non-nuclear military research and development facility in the town of Zelenograd, just north of Moscow, with all of its secret documents and arms prototypes. When confronted by the facility staff, the attackers claimed to work for a firm that had bought the company's stock and identified one member of their group as the new deputy director of the facility. Local Interior Ministry forces had to retake the facility from the men in an action reportedly involving hand-to-hand struggle and police firing automatic weapons into the air.[189]

The threat of insider theft at nuclear facilities and elsewhere in the former Soviet Union is also severe. In October 2004, sources in the local and regional Ministry of Internal Affairs reported that thieves had stolen three valves, valued at 700,000 rubles (over $20,000), from the Leningrad Nuclear Power Plant. The plant, like all Russian nuclear power plants, is protected by armed guards, leading police to assume that the theft was probably an inside job. Nor was this likely the first time such a theft has occurred: the head of the local branch of the Ministry of Internal Affairs told a reporter, "I don't know why this crime has attracted so much attention...such thefts happen here often."[190] Earlier in 2004, at the Rivne nuclear power plant in Ukraine, police broke up a ring that included four authorized workers and a

---

[187] Mark Deich, "The Ingushetia Knot," *Moskovskii Komsomolets*, 6 August 2004; Boris Yamshanov, "Bribes Reeking of Explosives," *Rossiiskaya Gazeta*, 16 September 2004.

[188] Peter Baker and Susan B. Glasser, "Russian Plane Bombers Exploited Corrupt System," *Washington Post*, 18 September 2004.

[189] Sergey Ptchikin, "Needles of Patriots: Attempts Made to Privatize Unique System for Protection Against Terrorists," *Rossiskaya Gazeta*, 21 December 2004.

[190] Andrey Pankov, "S Atomnoy Elektrostantsii Vynesli Tri Dorogostoyashchikh Klapana (Three High-Priced Valves Carried Off from Nuclear Power Plant)," *Novyye Izvestiya*, October 2004. This article is translated and summarized in "Three Pinch Valves Were Stolen from the Leningrad Nuclear Power Plant, Abstract 20040380," in *Nuclear Threat Initiative Research Library: NIS Trafficking Database* (Monterey, Cal.: Monterey Institute for International Studies, Center for Nonproliferation Studies, 2004; available at http://www.nti.org/db/nistraff/2004/20040380.htm as of 28 February 2005).

guard they bribed with $77 in Ukrainian currency; the group had successfully stolen a large steam evaporator worth an estimated $154,000 from inside the guarded plant.[191] (It is extraordinarily difficult to design a nuclear security system that will be effective in preventing theft by conspiracies of five insiders, including a guard, working together.) Insider theft of both money and weapons by military personnel continues to occur on epic scale; in 2003, for example, military prosecutors in Russia opened 14,000 criminal cases, including 1,700 crimes against federal property.[192] The Russian Audit Chamber has reportedly concluded that nuclear submarines arrive for decommissioning with half of their electronic equipment already stolen; theft of components from ships and submarines is so extensive that a gangland war broke out in Murmansk over the lucrative trade in stolen parts.[193] For these reasons, the 2004 CIA report repeatedly highlighted the insider danger.[194]

The temptations for such insider theft are high. As noted above, in one documented recent case, a Russian businessman was offering $750,000 for stolen weapon-grade plutonium for sale to a foreign client. Even though in this case the businessman linked up with scam artists and was caught, it seems unlikely that there is no one in Russia's vast nuclear infrastructure who could be convinced to provide plutonium in return for $750,000. The case is especially troubling because, rather than involving obvious foreigners attempting to purchase illicit items (such as the Aum Shinrikyo weapons-buyers), it involved a native Russian businessman, apparently with a foreign client interested in stolen plutonium, with enough savvy to make contact with people in one of the major closed cities where weapons-grade material is handled. This is a troubling indicator that those seeking nuclear weapons or materials may be making progress in closing the gap between them and people in Russia who may be willing to sell. Another troubling indicator is the large traffic in Afghan heroin being smuggled through Russia on its way to European markets – creating crime linkages and transport routes from the heart of Russia to Afghanistan and Pakistan that might be exploited for nuclear smuggling.[195]

Inadequate accounting of nuclear material in the past means that it will never be possible to know for sure how much material may already have been stolen. In his February 2005 testimony, CIA director Goss warned that in Russia "there is sufficient material

---

[191] See, for example, Oleg Bukharin, *Russia's Gaseous Centrifuge Technology and Uranium Enrichment Complex* (Princeton, N.J.: Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2004); Bukharin, *Surviving the End of the Cold War*. These and other sources are summarized in Center for Nonproliferation Studies, Monterey Institute for International Studies, "Thieves of Nuclear Plant Equipment Arrested in Ukraine," *NIS Export Control Observer* (May 2004; available at http://cns.miis.edu/pubs/nisexcon/pdfs/ob_0405e.pdf as of 5 March 2005).

[192] This was reported by Russia's chief military prosecutor in two interviews in the Russian state newspaper: "Not a Tin Soldier; Chief Military Prosecutor Comments on Investigation of Sensational Military Crimes," trans. BBC Monitoring, *Rossiskaya Gazeta*, 24 December 2003; "Business Breakfast [Interview with Col.-Gen. Alexander Savenkov]," trans. BBC Monitoring, *Rossiskaya Gazeta*, 27 December 2003.

[193] "'Enormous Damage' from Equipment Theft in Russian Navy," trans. BBC Monitoring Service, *RTR-TV (Moscow)*, 6 December 2003.

[194] U.S. National Intelligence Council, *Safety and Security of Russian Nuclear Facilities and Military Forces*.

[195] U.S. Department of State, "Europe and Central Asia: Russia," in *International Narcotics Control Strategy Report: 2003* (Washington, D.C.: U.S. Department of State, 2004; available at http://www.state.gov/p/inl/rls/nrcrpt/2003/vol1/html/29838.htm as of 17 December 2006).

unaccounted for so that it would be possible for those with know-how to construct a nuclear weapon," and pointed out that because some material was unaccounted for, he could not assure the American public that enough nuclear material for a bomb was not already in terrorist hands.[196] Russia is still transitioning from its Soviet-era nuclear material accounting system, designed to monitor production, not to detect theft. In essence, each facility measured its input and its output, and as long as the differences were small, they were written off as normal losses to waste – making it possible for careful thieves to steal nuclear material undetected day after day, as long as the individual thefts were small. (The chief engineer at one of Russia's major plutonium production sites reported that until cooperation with U.S. experts began, the accounting system at his site did not include the very concept of "material unaccounted for" – the difference between input and output was *defined* as "losses to waste."[197]) Over the decades of the Cold War, the few-percent uncertainties tolerated in this accounting system amount to many hundreds of bombs' worth of material that cannot be reliably accounted for.

To be fair, the U.S. nuclear material accounting system, though substantially better than the Soviet one (especially after new accounting measures were developed following the incident in which hundreds of kilograms of HEU were unaccounted for at the Nuclear Materials and Equipment Corporation (NUMEC) in the mid-1960s) was also not good enough during much of the Cold War to rule out the possibility that nuclear material had been stolen. When the United States published its plutonium inventory in the mid-1990s, some 2.8 tons of plutonium was "inventory differences" or "material unaccounted for."[198] For HEU, 3.2 tons of material fell into this category.[199] Probably these figures represent measurement uncertainities, material plated out on pipes, material lost to waste beyond that estimated to have gone to waste, and overestimates of how much was produced in the first place, but no one can demonstrate conclusively that none of it was stolen.

Today, at a number of sites in Russia where large quantities of nuclear material are processed every year, accounting has been much improved. But at many sites, there are still vast numbers of containers of nuclear material built up over decades, often sealed with seals that could be tampered with without detection, and no one has yet had the time and resources to measure each one to make sure that it still contains the nuclear material that the paper records say it should.

In short, the shape of the danger of nuclear theft from Russian facilities has changed in recent years – but the danger remains very real, and the need for action to ensure that every warhead and every kilogram of weapons-usable nuclear material in Russia is secure against both outsider and insider threats remains urgent.

---

[196] See Goss's testimony in *Current and Projected National Security Threats.*

[197] Interview, March 2001.

[198] U.S. Department of Energy, *Plutonium: The First 50 Years: United States Plutonium Production, Acquisition, and Utilization from 1944 Through 1994* (Washington, D.C.: DOE, 1996; available at http://www.fas.org/sgp/othergov/doe/pu50y.html as of 4 January 2007).

[199] U.S. Department of Energy, *Highly Enriched Uranium: Striking a Balance (Revision 1)* (Washington, D.C.: DOE, 2001; available at http://www.fas.org/sgp/othergov/doe/heu/striking.pdf as of 23 May 2006).

The Threat From Research Reactor Fuel

As indicated in Table 2.2, some 60 metric tons of HEU – enough for over a thousand nuclear weapons – is in civilian use or storage throughout the world. Most of this is in the form of fuel for research reactors. As noted earlier, more than 130 operating research reactors still use HEU as their fuel. An unknown number of shut-down or converted research reactors still have HEU fuel on-site. While a majority of these research reactors are either in the United States or Russia, all told, HEU-fueled reactors exist in some 40 countries. Indeed, for most of the countries in Table 2.3 and Table 2.4, the only separated plutonium or HEU on their soil is the HEU at one or a small number of research reactors.

Many of these facilities do not have enough HEU on-site for a bomb. But as noted above, a DOE study estimated that there are 128 nuclear research reactors or associated facilities around the world with 20 kilograms of HEU or more.[200] Moreover, one cannot rule out the possibility of terrorists stealing material from more than one facility, each of which might have less than the amount required for a bomb; the possibility of simultaneous attacks is highlighted by the simultaneous al Qaeda attacks on the U.S. embassies in Kenya and Tanzania in 1998. The potential use of research reactor HEU in nuclear weapons is not just a hypothetical concern: as discussed in the earlier section on demand for black-market nuclear material, Iraq, in its "crash program" to make one nuclear bomb as quickly as possible after its invasion of Kuwait, planned to use both fresh and irradiated HEU from its research reactors.[201]

Most civilian research reactors have very modest security – in many cases, no more than a night watchman and a chain-link fence even when enough fresh or irradiated HEU for a bomb is present.[202] Some are located on university campuses, where providing serious security against terrorist attack would be virtually impossible – and where the operators are often partly students, who cycle through frequently, making it extraordinarily difficult to provide serious checks of potential insider thieves. Many research reactors were built 30-40 years ago, in the heyday of nuclear energy; many have since fallen on hard times and have few resources to continue safe operation or to pay for substantial security measures. The research reactor in the Congo, attempting to operate in the midst of a civil war, at a facility so impoverished the reactor does not have a telephone, is emblematic of the broader problem (though its fuel is just below the 20% line that defines HEU): fuel stolen from that reactor turned up in the hands of the Italian mafia.[203]

---

[200] U.S. Congress, *DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium*, p. 28.
[201] For a detailed discussion based on the discoveries of the IAEA Iraq Action Team after the 1991 Gulf War, see Albright, Berkhout, and Walker, *Plutonium and Highly Enriched Uranium, 1996: World Inventories, Capabilities, and Policies*, pp. 344-349.
[202] Author's visits to research reactors in several countries. For a more detailed description of typical security arrangements at research reactors, see George Bunn et al., "Research Reactor Vulnerability to Sabotage by Terrorists," *Science and Global Security* 11 (2003; available at http://www.princeton.edu/~globsec/publications/pdf/11%202-3%20Bunn%20p85-107.pdf as of 2 January 2007).
[203] For a discussion of this episode, see Daly, Parachini, and Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor*.

Even in the United States, which has some of the most stringent nuclear security rules in the world for other facilities, research reactors regulated by the Nuclear Regulatory Commission (NRC) are exempted from the requirement that facilities with more than 5 kilograms of U-235 in HEU emitting less than 100 rads per hour at one meter must have sufficient armed guards, fences, and other security measures in place to defeat theft attempts by either an insider or groups of armed outsider attackers.[204] (This exemption and its implications are discussed at length in Chapter 4.) At the reactor at the Massachusetts Institute of Technology (MIT), since 9/11, there have been 1-2 Cambridge police officers with side-arms on-site to provide security. (Prior to the 9/11 attacks, the facility had no armed guards on-site, relying on response from off-site campus police officers in the event of a problem.) In April 2004, the facility had 29.5 kilograms of HEU on-site, which, prior to irradiation, had been 93% enriched.[205] To be fair, the MIT reactor is an unusually high-power research reactor (5 MWt), making the irradiated fuel there particularly radioactive and difficult to steal – but this is not true of many other research reactors that have similar security approaches. In mid-2005 an investigation by *ABC News* documented conditions ranging from sleeping guards to security doors propped open with books at essentially all of the 26 U.S. university-based research reactors.[206]

Given these security conditions, it would not be difficult for attackers to break in and remove large quantities of HEU from a research reactor, or for insiders to remove such material. Unlike the large and massive fuel assemblies used in nuclear power reactors, fuel for research reactors is typically in fuel elements that are small and easy to handle – typically less than a meter long, several centimeters across, and weighing a few kilograms. In most cases, a thief could easily put several fuel elements at a time into a backpack, to be carried out to a waiting vehicle.

In general, the HEU in these fuel elements would require some processing before it could be used in a bomb – but the kind of processing required is reasonably straightforward, and all the details of the necessary processes are published in the open literature. It is important to understand that the threat of nuclear theft at research reactors comes not only from the "fresh," unirradiated HEU fuel, but also from the irradiated fuel, which typically remains quite highly enriched; is much less radioactive than power reactor spent fuel (in many cases well below the 100 rad/hr level considered "self-protecting" against theft under international standards – a standard that should itself be reconsidered in the face of post-9/11 threats of suicidal attackers); and requires the same physical and chemical processing to recover HEU for use in a weapon as the fresh fuel elements require. (See Chapter 4 for an extended discussion of these points.) Thus, *kilogram for kilogram, lightly irradiated research reactor fuel poses only a modestly lower proliferation danger than fresh research reactor fuel* – and there is far more irradiated HEU fuel at poorly secured reactor sites around

---

[204] For a discussion, see, for example, Edwin Lyman and Alan Kuperman, "A Re-Evaluation of Physical Protection Standards for Irradiated HEU Fuel," in *The 24th International Meeting on Reduced Enrichment for Research and Test Reactors, Bariloche, Argentina, 5 November 2002* (Argonne, Ill.: Argonne National Laboratory, 2002; available at http://www.rertr.anl.gov/Web2002/index.html as of 16 May 2006).

[205] Visit by the author, April 2004.

[206] "Radioactive Road Trip," "PrimeTime Live," *ABC News*, 13 October 2005.

the world than there is fresh fuel.[207] The danger posed by research reactor spent fuel stands in stark contrast to the modest theft threat posed by nuclear power reactor spent fuel assemblies, which are huge, heavy, and intensely radioactive, making them quite difficult to steal and process.

Security of Pakistan's Stockpile

Pakistan has a relatively modest nuclear stockpile, which is thought to be distributed among only a small number of locations. Pakistan has sites where nuclear weapons exist (reportedly stored in partially disassembled form[208]) and sites with HEU or separated plutonium (particularly the main HEU production facility at Kahuta, but also including, among others, a research reactor with a small amount of U.S.-supplied HEU).[209] Pakistan's nuclear facilities are believed to be heavily guarded, though they probably are not equipped with state-of-the-art physical protection and material control and accounting technologies.[210]

Clearly, either state collapse or the rise of an extremist Islamic government in Pakistan – neither of which can by any means be ruled out – could pose severe dangers of nuclear assets becoming available to terrorists or hostile states. Even in the current environment, however, both insider and outsider threats to Pakistan's stockpiles appear to be dangerously high – creating serious dangers despite the relatively modest size and relatively high levels of security of Pakistan's nuclear stockpiles.

Insider threats. Recent events highlight the danger that insiders in Pakistan's nuclear complex, motivated by money, sympathy to extreme Islamic causes, or both, might help terrorists get a bomb or bomb material from Pakistan's stockpiles. First among these events are the extraordinary revelations concerning the global black-market nuclear network led by A.Q. Khan, the father of Pakistan's bomb, demonstrating that at least some nuclear insiders in Pakistan have been willing to sell practically anything to practically anyone – including

---

[207] For a discussion of these stockpiles, see Iain G. Ritchie, "Growing Dimensions: Spent Fuel Management at Research Reactors," *IAEA Bulletin* 40, no. 1 (March 1998; available at http://www.iaea.org/Publications/Magazines/Bulletin/Bull401/article7.html as of 20 September 2006). Some analysts have pointed to the modest interest that commercial reprocessing firms have had in separating uranium from research reactor fuel to argue that such separations would be very difficult. But there is a huge difference between separating enough uranium to be of commercial interest and separating the much smaller amount needed for a bomb – and there is a huge difference between separations that meet all modern safety regulations and quick and dirty separations that might be done by terrorists.

[208] See, for example, Lee Feinstein et al., *A New Equation: U.S. Policy toward India and Pakistan after September 11* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.ceip.org/files/pdf/wp27.pdf as of 4 October 2006). The chapter by Albright is of special interest.

[209] For a summary, see, for example, Joseph Cirincione, Jon B. Wolfsthal, and Miriam Rajkumar, *Deadly Arsenals: Nuclear Biological, and Chemical Threats*, 2nd ed. (Washington, D.C.: Carnegie Endowment for International Peace, 2005), pp. 239-258.

[210] The sparse information that is publicly available is summarized in Nathan Busch, *No End in Sight: The Continuing Menace of Nuclear Proliferation* (Lexington, KY: University Press of Kentucky, 2004). For a summary of which institutions within Pakistan are responsible for each aspect of nuclear security and accounting, see Muhammad Afzal, "Cooperation in Fissile Material Management: The View from Pakistan," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

designs and production manuals for uranium enrichment centrifuges, centrifuge components, operational centrifuges, and an apparently Chinese-origin nuclear bomb design.[211] The fact that the network was able to remove entire centrifuges from Pakistan's premier nuclear weapons material production facility and ship them off to other countries suggests either government approval or a truly extraordinary breakdown in security. Second, there is the remarkable case described earlier, in which Osama bin Laden and his deputy Ayman al-Zawahiri met at length with two senior Pakistani nuclear weapons experts with extreme Islamic views and pressed them both about nuclear weapons and about others in Pakistan's program who might be willing to help. Neither of these Pakistani scientists were ever tried or imprisoned, though it appears they remain under a loose form of house arrest. Bin Laden may have been on the right track in asking for others who could help: by one estimate from a Pakistani physicist, some 10% of Pakistan's nuclear insiders are inclined to extreme Islamic views.[212] Third, Pakistani investigations of the assassination attempts against President Musharraf in late 2003 suggest that they were carried out by military officers in league with al Qaeda operative Abu Faraj al-Libbi, raising the disturbing possibility that al Qaeda might also find people willing to cooperate among the officers charged with guarding nuclear stockpiles.[213] In short, the danger that insiders might pass material or weapons to al Qaeda, or facilitate an outsider attack, appears to be very real.

Outsider threats. Similarly, the threat from a possible terrorist attack on a Pakistani nuclear weapon depot appears dangerously high. Armed remnants of al Qaeda and of the Taliban continue to operate in the nearly lawless tribal zones on Pakistan's border with Afghanistan. Indeed, some combination of al Qaeda, Taliban, and Pakistani fighters was able to hold off thousands of Pakistani regular army troops for days at a time in a pitched battle in the tribal zones in early 2004.[214] If 41 heavily armed terrorists can strike without warning in the middle of Moscow, how many might appear at a Pakistani nuclear weapon storage site? Would the guards at the site be sufficient to hold them off – and would the guards choose to fight, or to cooperate?

A Global Threat

The identification of these three categories as the highest priority threats is by no means intended to minimize the threats that exist elsewhere around the world. There is probably no country where nuclear weapons and weapons-usable materials are located that does not have more to do to ensure that its nuclear stockpiles are secured and accounted for to a level sufficient to defeat demonstrated terrorist and criminal threats. This is a global problem, which can only be solved through a global partnership for nuclear security. Brief summaries of some of the other major stockpiles around the world follow below, beginning

---

[211] See, for example, the summary and references in Braun and Chyba, "Proliferation Rings."
[212] Neuffer, "A US Concern: Pakistan's Arsenal: Anti-American Mood Poses a Security Risk."
[213] "Escaped Musharraf Plotter Was Pakistan Air Force Man," *Agence France Presse*, 12 January 2005; "Musharraf Al-Qaeda Revelation Underlines Vulnerability: Analysts," *Agence France Presse*, 31 May 2004.
[214] See, for example, Afzal Khan, "Pakistan's Hunt for Al Qaeda in South Waziristan," *The Jamestown Foundation*, 22 April 2004 (available at http://www.jamestown.org/news_details.php?news_id=45 as of 5 December 2005).

with the developing countries that possess nuclear weapons; continuing to the developed countries that possess nuclear weapons; and then considering the problem of civilian separated plutonium (civilian HEU having been discussed above).

China. While public information about China's approaches to nuclear security and accounting is sparse, China's nuclear security system is believed to be heavily dependent on "guards, guns, and gates," as the Soviet system was, with relatively little application of modern safeguards technologies.[215] China does not have a specific DBT defined in regulations, and systematic engineering approaches to assessing and correcting vulnerabilities are typically not applied.[216] Chinese experts have expressed concern that improved protections against insider theft may be needed as China shifts toward a more market-oriented (and more corrupt) society.[217] Outside terrorist attack may someday also be an issue: China does have a continuing problem with terrorist groups, including groups based in China's Islamic minority, which the Chinese government believes are linked to al Qaeda. The United States and China initiated a lab-to-lab cooperation program on technologies for securing and accounting for nuclear materials in the late 1990s, which ultimately included the installation of a demonstration facility for modern safeguards and security technology at the China Institute of Atomic Energy in Beijing, which U.S. participants hoped would create a new standard for securing and accounting for nuclear materials in China.[218] This cooperation was cut off after the scandal over allegations of Chinese nuclear espionage in the United States. Recently, cooperation with respect to civilian nuclear material has resumed, and extensive upgrades of protection, accounting, and control technologies were completed at one site in the fall of 2005, as a demonstration. U.S.-Chinese cooperation on a broad range of physical protection, material control, and material accounting issues in China's civil sector is now underway, but this cooperation typically does not involve U.S. funding for installing extensive

---

[215] For a summary of MPC&A in China, see Hui Zhang, "Evaluating China's MPC&A System," in *Proceedings of the 44th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 13-17 July 2003* (Northbrook, Ill.: INMM, 2003; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/MPC&A.pdf as of 1 August 2005). See also the summaries of the sparesparse publicly available literature in Nathan Busch, "China's Fissile Material Protection, Control, and Accounting: The Case for Renewed Collaboration," *Nonproliferation Review* 9, no. 3 (Fall-Winter 2002; available at http://cns.miis.edu/pubs/npr/vol09/93/93busch.pdf as of 1 August 2005); Busch, *No End in Sight: The Continuing Menace of Nuclear Proliferation.*

[216] Tang Dan, "Physical Protection System and Vulnerability Analysis Program in China: Presentation to the Managing the Atom Seminar" (23 March 2004). In an interview in October 2006, a Chinese physical protection regulator confirmed that at most sites, a systematic vulnerability assessment has not yet been performed.

[217] See Tang Dan et al., "Physical Protection System and Vulnerability Analysis Program in China," in *Eu-High Level Scientific International Conference on Physical Protection* (Salzburg, Austria: Austrian Military Periodical, 2002; available at http://www.numat.at/list%20of%20papers/tangdan%20-%20unkorrigiert.pdf as of 5 April 2006). (It is notable that the authors begin with a review of recent changes in Chinese society, with the conclusion that these changes increase the criminal threat and decrease the ability to rely solely on the loyalty of insider personnel.)

[218] See Nancy Prindle, "The U.S.-China Lab-to-Lab Technical Exchange Program," *Nonproliferation Review* 5, no. 3 (Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/prindl53.pdf as of 11 May 2006).

upgrades (as it has in Russia), and as of late 2006, cooperation on these issues with China's military nuclear sector had not resumed.[219]

India. In India's case, like China's, the amount of information about actual nuclear security practices which is publicly available is small.[220] Nuclear weapons and weapons-usable nuclear material are believed to be located in a small number of facilities under heavy guard. A special security force, the Central Industrial Security Force (CISF), guards both nuclear installations and other especially dangerous or sensitive industrial facilities. Indian experts report that India does perform systematic vulnerability assessments in designing physical protection systems for nuclear facilities and does use some modern security technologies, including access controls and various types of intrusion detectors.[221] Resources available for physical protection appear to be limited, however, and in some cases physical protection systems are aging and have some important weaknesses.[222] The widespread government corruption in India, coupled with past incidents such as the assassination of a Prime Minister by her own guards, suggests that potential insider threats should be taken seriously. And repeated terrorist attacks, including on defended facilities such as military bases (and the Indian Parliament) suggest that protection must also be provided against potentially substantial outsider attacks.

North Korea. North Korea has announced that it has manufactured nuclear weapons and tested a weapon in the fall of 2006 (though it achieved a yield assessed by U.S. intelligence at less than a kiloton). North Korea may have sufficient separated plutonium for 2-9 bombs.[223] Almost nothing is known about this stockpile or its security arrangements,

---

[219] For discussions of the recent upgrade, see U.S. Department of Energy, National Nuclear Security Administration, "U.S. And China Jointly Host Technology Exposition on Nuclear Material Security and International Safeguards: Collaborative Approaches to Enhancing Nuclear Material Security" (Washington, D.C.: NNSA, 24 October 2005; available at http://www.nnsa.doe.gov/na-20/docs/china_tech_demo.pdf as of 24 February 2006); Stephen Wampler, "DOE Helps Chinese Agency to Secure Nuclear Material," *Lawrence Livermore National Laboratory's Weekly Newsline*, 16 December 2005 (available at http://www.llnl.gov/pao/employee/articles/2005/12.16.05.newsline.pdf as of 24 February 2006).Supplemented by interviewsInterviews with DOE officials, December 2004, April 2005, and July 2005, and October 2006.

[220] Some additional detail was provided at International Atomic Energy Agency, "IAEA Regional Training Course on Security for Nuclear Installations," Mumbai, India, 11-20 May 2003. For a summary of other publicly available information, see Busch, *No End in Sight: The Continuing Menace of Nuclear Proliferation.*

[221] See presentations to International Atomic Energy Agency, "IAEA Regional Training Course on Security for Nuclear Installations."

[222] Interview with U.S. expert who toured the physical protection system at an Indian power reactor, at Indian invitation, in 2003. Personal communication, July 2003.

[223] See, for example, David Albright and Paul Brannan, "The North Korean Plutonium Stock, Mid-2006" (Washington, D.C.: Institute for Science and International Security, 26 June 2006; available at http://www.isis-online.org/publications/dprk/dprkplutonium.pdf as of 13 August 2006).[223] See, for example Albright and Brannan, "The North Korean Plutonium Stock, Mid-2006". Albright and Brannan estimate that as of mid-2006, North Korea had 20-53 kilograms of separated plutonium. If North Korea required the same amount of plutonium per weapon as was used in the Nagasaki bomb, about six kilograms, and sufferssuffered 20% losses in processing of its separated plutonium into weapons (so that 7.5 kilograms of plutonium would be needed to end up with 6 kilograms in a bomb), this amount of separated plutonium would be sufficient for 2-7 nuclear weapons. If North Korea has succeeded in designing its weapons to use less plutonium, and in reducing processing losses, the number of weapons might be somewhat higher; at five kilograms per bomb and 10%

though it is presumed that wherever these materials or weapons are, they are heavily guarded. Given North Korea's extreme isolation, it is extremely unlikely that modern technologies for access control, intrusion detection, barriers, and the like are currently used. North Korea's stockpile is presumably carefully watched and is sufficiently small that it would probably be effectively impossible for an insider to remove enough material for a bomb without detection – though the possibility of a corrupt cabal of senior military or party officials deciding to sell off material cannot be excluded. Given the highly controlled nature of North Korean society, a substantial outsider attack on these facilities in peacetime also seems quite unlikely. Concerns about this stockpile falling into the hands of terrorists usually focus on either (a) a conscious decision by the North Korean state (or by senior nuclear officials) to sell nuclear material or weapons;[224] or (b) a "loose nukes" scenario in the event of a collapse of the North Korean regime.[225] Installing improved nuclear security and accounting equipment would not address either of those concerns. Successful engagement with the North Korean government that convinced it to verifiably eliminate all of its nuclear programs, however, would remove the nuclear weapons and weapons-usable materials that might otherwise be transferred or fall out of state control.[226]

Israel. Israel's nuclear stockpile is believed to exist at a very small number of sites, under heavy guard, but as Israel does not even officially acknowledge that the stockpile exists, virtually no details of its security arrangements are publicly available. Israel has long experience in battling terrorist threats and a reputation for taking harsh measures against those involved in security breaches (as in the case of former nuclear weapons worker Mordechai Vannunu). This suggests that Israel has probably put in place substantial security measures for its nuclear stockpile.

The United Kingdom. Britain requires every facility with nuclear weapons or weapons-usable nuclear material to have security in place sufficient to meet a specified DBT; armed guards are employed to protect nuclear weapons and weapons-usable nuclear material

---

losses, for example, 53 kilograms would be enough for roughly 10 bombs. Since one weapon has been detonated, one must be subtracted from any estimated total; hence the 2-9 figure in the text. Albright and Brannan assume only 4-5 kilograms of plutonium per weapon, and assume that the only processing losses occur in separating the plutonium from irradiated fuel, so that the 20-53 kilograms would be sufficient for 4-13 weapons. I believe the assumption of zero processing losses in fabrication is unrealistic, and that 10-20% is a more realistic figure.

[224] On some occasions, representatives of the North Korean regime have reportedly made vague hints threatening to transfer nuclear weapons or materials; on other occasions, they have pledged never to allow nuclear material or weapons to be transferred. See, for example, statements quoted in Selig Harrison, "Inside North Korea: Leaders Open to Ending Nuclear Crisis," *Financial Times*, 4 May 2004 (available at http://ciponline.org/asia/inside.htm as of 17 December 2006). North Korea would presumably understand that U.S. retaliation would be overwhelming if the material for a terrorist nuclear strike were reliably traced back to North Korea. Nevertheless, concern persists over the possibility of such a transfer.See Chapter 3 for a more extended discussion of the possibility of conscious state transfer of nuclear weapons or materials to terrorists, and how large a contribution to the overall risk of nuclear terrorism this may make.

[225] See, for example, Ashton B. Carter, William J. Perry, and John M. Shalikashvili, "A Scary Thought: Loose Nukes in North Korea," *Wall Street Journal*, 6 February 2003.

[226] For a discussion, see "Keeping North Korean Bomb Material Out of Terrorist Hands," in Bunn and Wier, *Securing the Bomb: An Agenda for Action*, pp. 32-33.

(though armed guards were only dispatched to protect nuclear power plants in 2005[227]); regular vulnerability assessments are carried out, and modern physical protection and material control and accounting technologies are in place. Significant improvements in physical protection have been made since the 9/11 attacks.[228] The British view as to the level of spending required to provide sufficient security is quite different from the U.S. view, however. As of 2000, for example, security spending to protect and safeguard the plutonium at the Sellafield site (a huge complex processing tons of weapons-usable separated plutonium every year and with tens of tons of separated plutonium in storage on-site) were in the range of £10 million per year[229] (approximately $18 million 2007 dollars) – compared to over $100 million per year the United States was spending on securing Los Alamos during the same period.[230] In 1998, the plutonium and HEU reprocessing plant at Dounreay dramatically failed a security test when a mock attack force rapidly defeated the site's defenses, and the chief of the UK Atomic Energy Constabulary (the guard force for nuclear facilities) resigned, charging that he had been unable to get authorization to hire enough guards to provide effective security.[231] In 2002 and 2003, Greenpeace protesters were able to get past the security fences at the Sizewell B nuclear power reactor, climb the reactor building with ladders, and get through an unsecured fire door into an inner secure area (though not to vital areas where equipment whose sabotage could cause a major accident is located). While this does not necessarily reflect what would happen in the event of a terrorist attack, as the guards obviously take a different approach to protesters than they would to armed attackers, Britain's nuclear security regulator acknowledged that the incident "should not have been possible," and expressed particular concern over the fire door not having been secured between the first incursion and the second.[232]

---

[227] Pearl Marshall, "U.K. Upgrading Nuclear Security by Posting Armed Police at Sites," *Nucleonics Week* (27 January 2005).

[228] For a useful recent summary of publicly available information on nuclear security in the United Kingdom, see Parliamentary Office of Science and Technology, *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*, vol. Report 222 (London: POST, 2004; available at http://www.parliament.uk/documents/upload/POSTpr222.pdf as of 2 August 2005). See also BNFL National Stakeholder Dialogue, Security Working Group, *Final Report* (London: The Environment Council, 2004).

[229] See Appendix 3 in BNFL National Stakeholder Dialogue, Waste Working Group, *Interim Report* (London: Environmental Council, 2000; available at http://www.the-environment-council.org.uk/docs/WWG%20Combined%20Report.pdf as of 4 August 2005).

[230] See U.S. Department of Energy, *Fiscal Year 2003 Budget Request: Detailed Budget Justifications—Weapons Safeguards and Security* (Washington, D.C.: DOE, 2002; available at http://www.cfo.doe.gov/budget/03budget/content/weapons/OthrWeap.pdf as of 4 August 2005).

[231] Dave King and Steve Smith, "Doomed Nuke Plant Dogged by Trouble," *Scottish Daily Record*, 5 June 1998; Angela Jameson, "Elite Armed Force Stands Firm after Nuclear Shake-Up: The Saturday Interview: Bill Pryke," *The Times*, 14 August 2004; Roger Hannah, "Dounreay Security Has Been Dodgy for Years," *Scottish Daily Record*, 28 April 1998.

[232] See discussion in Director of Civil Nuclear Security, *The State of Security in the Civil Nuclear Industry and the Effectiveness of Security Regulation: April 2002 – March 2003* (London: Office for Civil Nuclear Security, Department of Trade and Industry, 2003; available at http://www.dti.gov.uk/files/file23303.pdf?pubpdfdload=03%2F418 as of 28 July 2006). See also Parliamentary Office of Science and Technology, *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*, p. 33.

France. As in Britain, in France sites with nuclear weapons and weapons-usable nuclear materials are required to be able to defend against a specified DBT, and both armed guards and modern safeguards and security technologies are employed. Significant additional security steps have been taken since 9/11; for some weeks after those attacks, air-defense missiles were deployed outside the reprocessing plant at La Hague.[233] But as in other countries, concerns over security weak points remain. Nuclear power plants in France, which often have unirradiated plutonium-uranium mixed oxide (MOX) fuel on-site, have no armed guards on-site.[234] The frequent transports of weapons-usable separated plutonium in France are a particular concern. Greenpeace, for example, has repeatedly been able to track the supposedly secret routes of plutonium transport trucks. In February 2003, Greenpeace protesters succeeded in surrounding one of these trucks, which was carrying 150 kilograms of separated plutonium at the time; had they been armed terrorists, it appears likely that they would have succeeded in seizing the trucks and their contents (though as in other such cases, the authorities point out that the guards' reaction to unarmed protesters is inevitably far different from their reaction to a terrorist attack).[235] A recent analysis of security arrangements for transport of civilian plutonium by a former security specialist for DOE, commissioned by Greenpeace and based on photographs of the security arrangements provided by Greenpeace, concluded that the risks were worse than what would be considered "high" (and therefore unacceptable) in the DOE system and dubbed them "extreme."[236]

United States. The United States may have the most stringent nuclear security rules in the world and almost certainly spends more on securing its nuclear stockpiles than any other country. Annual safeguards and security spending at DOE alone is now in the range of $1.5 billion per year;[237] the private sector and the Department of Defense spend hundreds of millions more each year. All facilities with nuclear weapons or weapons-usable nuclear material are required to be able to defeat a specified DBT; both armed guards and modern safeguards and security technologies are used to protect these sites (and to protect transports). Regular performance tests probing facilities' ability to fend off mock attackers are required. While details are classified, the DBT now in place for nuclear weapons and weapons-usable nuclear material at DOE is reported to be comparable in magnitude to the 19 attackers in four independent, well-coordinated groups that struck on 9/11.[238] Nevertheless, even in the United States there have been repeated controversies over whether nuclear facilities are adequately

---

[233] See discussion, for example, in Parliamentary Office of Science and Technology, *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*, p. 38.

[234] See discussion, for example, in Parliamentary Office of Science and Technology, *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*, p. 38.

[235] [235] Greenpeace International, "The Action in Chalon: Greenpeace Blocks Plutonium Traffic" (19 February 2003; available at http://www.greenpeace.fr/stop-plutonium/en/20030219_en.php3 as of 5 May 2006).

[236] Timm, *Security Assessment Report for Plutonium Transport in France.*

[237] U.S. Department of Energy, *FY 2007 Congressional Budget Request: Other Defense Activities*, vol. 2, DOE/CF-003 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_2_ODA.pdf as of 22 December 2006), p. 161.

[238] For a useful discussion of the several steps in the evolution of DOE's DBT since 9/11, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Y-12 and Oak Ridge National Laboratory at High Risk* (Washington, D.C.: POGO, 2006; available at http://pogo.org/p/homeland/ho-061001-Y12.html as of 17 November 2006).

secured and repeated cases of security tests revealing serious vulnerabilities in physical protection and accounting systems for nuclear material in the U.S. nuclear complex.[239] A number of the major security initiatives DOE is now undertaking – particularly the consolidation of nuclear materials into fewer, more secure locations – have been slowed by opponents who question their cost and value.[240]

As noted earlier, HEU at NRC-regulated research reactors is exempt from most of the security requirements that the same material would require if it was located anywhere other than a research reactor. Lightly irradiated HEU is exempt from nearly all of the NRC's security requirements. Tons of HEU metal – the easiest material in the world for terrorists to use to make a nuclear bomb – exists at two NRC-licensed facilities that are required to defend against a far smaller and less capable DBT than DOE sites handling the same material would be required to defend against.[241] The NRC has recently ruled that reactors using plutonium in MOX fuel can be exempted from a substantial fraction of the security requirements that are required at other sites with weapons-usable nuclear material, arguing that there is "no rational reason" why a reactor with potential nuclear bomb material on-site should have any more security than any other reactor.[242] DOE's security rules exempt a wide range of types of material that pose serious security risks from major security requirements, including most HEU research reactor fuel. DOE's rules define any material that has less than 10% by weight

---

[239] For a blistering critique of security in the U.S. nuclear weapons complex, published shortly after the 9/11 attacks, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Security at Risk* (Washington, D.C.: POGO, 2001; available at http://www.pogo.org/p/environment/eo-011003-nuclear.html as of 4 December 2006). For a recent summary of progress made in improving security since then and problems still remaining, including both official views and those of critics, see Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *A Review of Security Initiatives at DOE Nuclear Facilities*, U.S. Congress, House of Representatives, 109th Congress, 1st Session, 18 March 2005 (available at http://energycommerce.house.gov/108/Hearings/03182005hearing1457/hearing.htm as of 15 August 2005). For a brutal earlier official review (including a long history of past negative assessments), see President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington D.C.: PFIAB, 1999; available at http://www.fas.org/sgp/library/pfiab/ as of 13 December 2006).

[240] See *A Review of Security Initiatives at DOE Nuclear Facilities*. For a useful discussion of the opportunities for and obstacles to consolidation, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006).

[241] The two sites are Nuclear Fuel Services, in Erwin, Tennessee and the Nuclear Productions Division of BWXT Technologies, in Lynchburg, Virginia. See, for example, the brief mention of this point in Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities*.

[242] U.S. Nuclear Regulatory Commission, *In the Matter of Duke Energy Corporation (Catawba Nuclear Station, Units 1 and 2)*, CLI-04-29 (Washington, D.C.: NRC, 2004; available at http://www.nrc.gov/reading-rm/doc-collections/commission/orders/2004/2004-29cli.pdf as of 22 September 2006); U.S. Nuclear Regulatory Commission, *NRC Authorizes Use of Mixed Oxide Fuel Assemblies at Catawba Nuclear Power Plant* (Washington, D.C.: NRC, 2005; available at http://www.nrc.gov/reading-rm/doc-collections/news/2005/05-043.html as of 30 December 2006).

U-235 as falling outside Category I, which is the only category that requires stringent security measures.[243] (These issues are discussed at length in Chapter 4.)

The plutonium powers. Several European states, Japan, Russia, and (to a lesser extent) India reprocess their civilian spent fuel to separate the plutonium for use as new fuel. (China plans to do so as well, but has not yet begun civilian reprocessing on any substantial scale.) Despite the remarkable progress of safeguards and security technologies in recent decades, a world in which tens of tons of separated, weapons-usable plutonium are being processed and shipped from place to place every year – when only a few kilograms are needed for a bomb – inevitably involves greater risks of nuclear theft and terrorism than would a world in which this was not occurring.[244] The British Royal Society, in a 1998 report, warned that even in an advanced industrial state like the United Kingdom, the possibility that plutonium stocks might be "accessed for illicit weapons production is of extreme concern."[245]

In Britain, France, and non-nuclear-weapon states such as Japan and Germany, this material is under international safeguards and is therefore accounted for to international standards – but these safeguards are designed only to detect whether the host state might be diverting civilian material for military purposes, not to prevent theft. Standards for security vary widely from one country to the next and are generally lower for this civilian material than they are for military materials. In Japan, for example, as noted earlier, armed guards were not required for plutonium facilities before 9/11, and the armed units of the national police deployed to protect these sites since then are reportedly not well integrated into the sites' overall security plans. Japan has just approved a new nuclear security law, but guards at nuclear sites are still only required to be armed with billy clubs, raising obvious questions as to how the sites can meet new requirements to be able to hold off attackers until off-site response forces arrive.[246] As noted earlier, in France, reactors where plutonium fuel is present,

---

[243] For the specifics of categorizing different types of material, current DOE orders still refer back to U.S. Department of Energy, *Guide to Implementation of DOE 5633.3b, "Control and Accountability of Nuclear Materials"* (Washington, D.C.: DOE, 1995).

[244] While this plutonium is largely "reactor-grade," all separated plutonium (except plutonium with 80% or more of the isotope Pu-238) is weapons-usable. Terrorists or unsophisticated states could make a crude bomb from reactor-grade plutonium, using technology no more sophisticated than that of the Nagasaki bomb, which would have an assured, reliable yield in the kiloton range (and therefore a radius of destruction roughly one-third that of the Hiroshima bomb) and a probable yield significantly higher than that; sophisticated states could make weapons with reactor-grade plutonium that would have similar yield, weight, and reliability to those made from weapon-grade plutonium. For an authoritative unclassified discussion, see U.S. Department of Energy, Office of Arms Control and Nonproliferation, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*, DOE/NN-0007 (Washington, D.C.: DOE, 1997; available at http://www.osti.gov/bridge/servlets/purl/425259-CXr7Qn/webviewable/425259.pdf as of 2 January 2007). For further discussion and references, see Chapter 4.

[245] The Royal Society, *Management of Separated Plutonium* (London: Royal Society, 1998; available at http://www.royalsoc.ac.uk/displaypagedoc.asp?id=18551 as of 17 December 2006).

[246] See, for example, Hiroshi Masumitsu, "Revised N-Law Inadequate to Cover All Terrorism Scenarios," *Daily Yomiuri*, 18 June 2005. The armed guards currently present at nuclear sites in Japan have been deployed there at the expense of the national police, and are not required by regulation; they may be removed at any time. Interview with Japanese physical protection regulator, November 2006.

like other reactors, have no on-site armed guards. U.S. experts visiting the Belgian plutonium fuel fabrication facility in the mid-1990s found it lightly guarded.[247]

[247] Personal communication from Frank von Hippel, 1996.

3. The Risk of Nuclear Terrorism: A Mathematical Model

No one can reliably calculate the size of the risk of nuclear terrorism, or the effectiveness of alternative policies to reduce that risk. The factors that affect the risk are simply too uncertain (and probably changing).

The use of a mathematical model cannot eliminate these uncertainties, but it can make assumptions about the key factors affecting the risk explicit and thus focus debate; provide a tool for assessing the effectiveness of alternative policies; and focus efforts to collect additional information to reduce the uncertainties in estimating the values of the model parameters. In Chapter 2, a qualitative description of the factors affecting the risk of nuclear terrorism supported an argument that the risk is substantial and justifies urgent action to reduce it. In this chapter, I propose a simple mathematical model of the risk of nuclear terrorism (with risk defined as the probability of a nuclear terrorist attack times its consequences); offer a numerical example; and then discuss each parameter, assessing what information may be available to help understand what its value may be, what policy options are available for changing it, and what additional information might be collected that would reduce the uncertainty in estimating the value of that parameter.

This model goes well beyond previous publicly available models of nuclear terrorism, which have generally focused on the engineering aspects and almost left the terrorists themselves out of the equation, assuming that the risk scaled linearly with either the quantity of material or the number of facilities where such material could be stolen.[1] This chapter provides the first published model of nuclear terrorism risk that responds realistically to variations in each of the parameters. Among the key insights that will be developed from the model and the discussions of its input parameters in this chapter are the following:

- Plausible estimates of the values of the input parameters can support published estimates of a 30-50% ten-year probability of a terrorist nuclear detonation. (The numerical example of the use of the model in this chapter leads to an estimate of 29% for this 10-year probability.) Only extremely optimistic estimates of the parameter values would support estimates of this 10-year probability in the range of 1%, which have been made by some authors.
- The model suggests that the most effective interventions to reduce the risk of nuclear terrorism are likely to occur early in the pathway to nuclear terrorism. Counter-terrorism

[1] For a simple model where the risk a material poses simply goes up linearly with the quantity of material, see Edwin Zebroski, "Analysis of Risks of Diversion of Plutonium or Highly Enriched Uranium," reproduced in Committee on Science, Space, and Technology, *Conversion of Research and Test Reactors to Low-Enriched Uranium (LEU) Fuel*, U.S. Congress, House of Representatives, 98th Congress, 2nd Session, 25 September 1984, pp. 60-74. For a model in which the risk of nuclear theft and terrorism increases linearly with the number of sites where weapons-usable nuclear materials exist, see Roger E. Avedon, "On the Future of Civilian Plutonium: An Assessment of Technological Impediments to Nuclear Terrorism and Proliferation" (Ph.D. dissertation, Engineering Economic Systems and Operations Research, Stanford, 1997).

efforts that were only modestly effective, resulting in only small reductions in the number of plausible nuclear terrorist groups and in the effectiveness of the remaining groups, could result in substantial reductions in the risk of nuclear terrorism. Improvements in nuclear security measures that cut the probability of both outsider and insider theft by a substantial fraction could greatly reduce the overall risk.

- Despite the possibility that some of the risk comes from nuclear material that has already been stolen, nuclear security improvements for the not-yet-stolen material would result in large reductions in overall risk unless the fraction of the risk of black-market acquisition resulting from already-stolen material was unrealistically high and the fraction of the time terrorists chose to attempt to get material by instigating new thefts was very low.

A key insight developed in this chapter (not from the model itself from the consideration of the values of the input parameters to it) is that what is important about nuclear security is neither the *average* security level nor the *average* adversary capability employed in a nuclear theft attempt, but the tails of these distributions. By far the highest risks of successful nuclear theft arise when an unexpectedly capable terrorist or criminal group attempts to steal material from one of the most vulnerable facilities. Modest investments in improving security at those few nuclear facilities and transport legs where security is weakest and the threats are highest may be able to reduce the probability of successful nuclear theft substantially.

Choosing a Modeling Approach

A wide range of models have been or could be applied to modeling terrorism risks. The choice of approach is complicated by the fundamental difference between terrorism risks and accident risks, which is that terrorist attacks are the result of conscious decisions by intelligent and adaptive adversaries, rather than random events.

The approach that should be chosen in building a model of the terrorism problem depends on what aspects of the problem the model is intended to illuminate. If the purpose is to elucidate *terrorist decision-making and target selection*, then modeling approaches focused on decision-making and behavior should be used. Some analysts, for example, have used game-theoretic models portraying the problem as a strategic game in which terrorists are seeking to maximize the consequences of their attacks, and governments are attempting to minimize the consequences of those attacks.[2]

---

[2] See, for example, Gordon Woo, "Quantitative Terrorism Risk Assessment," *Journal of Risk Finance* 4, no. 1 (October 2002; available at http://www.rms.com/NewsPress/Quantitative_Terrorism_Risk_Assessment.pdf as of 22 May 2006). Woo and his company, Risk Management Solutions, have developed a proprietary model used in the insurance industry to estimate different types of terrorism risks to insured assets (including, among others, the risk of nuclear terrorism). The structure of the model is game-theoretic, but the estimates of the probability of success for particular types of terrorist attack (such as terrorists' ability to get nuclear materials and make them into a nuclear bomb) rely heavily on solicitation of expert opinion. Woo's articles do not discuss the specifics of the model in any detail; somewhat more information on the model can be found in an assessment of terrorism risks that makes use of the model, in Henry H. Willis et al., *Estimating Terrorism Risk* (Santa Monica, Cal.: RAND, 2005; available at http://www.rand.org/pubs/monographs/2005/RAND_MG388.pdf as of 6 May 2006). Important complications that could be added to such game-theoretic approaches include the possibility

Such models, however, often implicitly or explicitly assume that terrorists and those protecting against them are rational actors (within the framework of their own objectives), which may or may not be the case. To address that weakness of the game-theoretic models, others have argued that models based on data from the history of real terrorist networks – perhaps integrated into a social network analysis – will be more useful than abstract utility-maximizing models in understanding terrorist behavior and assessing the probabilities of different types of attacks in the future.[3] In some cases, either of these types of models can be dynamic, modeling the way that terrorists and the societal efforts to respond to them or protect against them in different countries might respond to each other and to external events over time.

If, on the other hand, the goal is to elucidate *the probability that various types of terrorist attack would succeed, and the likely consequences*, then the most appropriate and frequently used models are based on what is known as vulnerability assessment, a static approach very similar to probabilistic risk assessment (PRA).[4] Such approaches are typically used to assess the vulnerability of particular facilities to attacks using a particular level of terrorist capability (often specified in regulation as a "design basis threat" or DBT – that is, the threat that should be the basis for designing the facility security system). Just as a PRA asks: "What can go wrong? What is the likelihood of that happening? What are the consequences if it does happen?" a vulnerability assessment asks: "What could an adversary cause to go wrong? What is the likelihood the adversary would attempt to take that action, and would succeed? What are the consequences if it does happen?" Just as PRAs are based

---

that terrorist attackers might have very different assessments of the value of different consequences than the defenders (for example, placing a very high value on a successful attack on a highly symbolic target, even if this did not cause very much damage if measured in lives and economic value lost); that terrorists might have very different beliefs about the probability of success of different approaches than the defenders do; and that the terrorists might be either risk-prone or risk-averse (for example, putting a higher premium on certainty of success than a simple "maximizing expected consequences" approach might indicate). For discussion, see, for example, Mark K. Snell, "Estimation of Probability of Adversary Mission Success," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).

[3] See, for example, Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004). Sageman elaborated on the opportunities offered by a network analysis approach, and provided some examples of the use of this approach to analyze particular incidents, in his presentation "Threat Convergence: The Future of Terrorism Research," at the conference on "Threat Convergence," Fund for Peace, Washington, D.C., 7 April 2006. (The title "threat convergence" refers to the potential convergence of terrorism, weak or failed states, and weapons of mass destruction.)

[4] For general introductions to vulnerability assessment, see, for example, Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems* (Woburn, Mass.: Butterworth-Heineman, 2001); Byron Gardner, "Process of System Design and Analysis," paper presented at Workshop on Physical Protection, Moscow, 11-14 September 1995 (available at http://www.osti.gov/bridge/servlets/purl/112931-7hNczP/webviewable/112931.pdf as of 9 January 2007). For a critique, focusing on the difficulty of adequately accounting for complex system interactions and for unexpected adversary tactics, see Matthew Bunn, "Systems Approaches to Security for Nuclear Materials and Facilities", Presentation, "Research Seminar in Engineering Systems," Massachusetts Institute of Technology (Cambridge, Mass.: Managing the Atom Project, Harvard University, 4 December 2001). For a broader discussion of the application of modifications of quantitative risk assessment techniques to terrorism risks, see B. John Garrick, "Perspectives on the Use of Risk Assessment to Address Terrorism," *Risk Analysis* 22, no. 3 (June 2002).

on laying out a range of possible scenarios linking an initiating event or series of events to undesirable consequences, so a vulnerability assessment is based on laying out a range of possible scenarios that connect initiating events terrorists might cause to undesirable end states, with the complete sequence of events linking these, and estimates of the likelihood that terrorists would succeed in carrying out the various steps on each potential pathway.[5] Typically, vulnerability assessments are used to identify the most vulnerable pathways for a terrorist attack at a particular facility, *assuming that an attack does occur* – that is, the pathways offering terrorists with a given level of capability the highest chance of success in causing the undesired end-states – and then to design measures to reduce those most-urgent vulnerabilities.[6] Just as PRA has contributed to major improvements in safety in the nuclear industry and in other complex systems, the vulnerability assessment approach has contributed to large improvements in security at nuclear facilities and in recent years has been widely applied to assessing and reducing vulnerability of a wide range of facilities.

The model presented in this chapter takes the static approach of vulnerability assessment, extending it from looking at particular facilities to examining the entire pathway from a terrorist decision to attempt to get and use a nuclear bomb to the detonation of such a bomb. It takes this approach because its principal goal is to provide a structure for thinking through the different pathways terrorists might take to the bomb, and the factors that determine the probabilities that those pathways would succeed, if chosen. I have not attempted to marry this static model to any dynamic model of how terrorists would make their choices and how the choices at each step on the pathway might be affected by the results of previous steps, for three reasons. First, so little is known about how terrorists might make decisions about nuclear acquisition that explicit modeling of that decision-making process – as opposed to simply rough estimates of the likelihood that terrorists would choose different pathways, based on what little is known about their nuclear pursuits in the past – does not appear likely to offer significant additional understanding of the problem. Second, what little *is* known about the past record suggests that terrorists do *not* necessarily choose the paths that a game-theoretic approach focused on maximizing the probability of success would predict: Aum Shinrikyo's decision to try to get a nuclear bomb by the singularly unpromising pathway of purchasing a sheep farm in Australia to mine its own uranium for later enrichment – when it was operating in a country where hundreds of kilograms of highly enriched uranium (HEU) and plutonium were very lightly guarded at the time – is an obvious example. Third, terrorists in general will face even greater uncertainties than modelers do about what the best approaches to getting nuclear material and to building a nuclear bomb would be, and it is effectively impossible to predict what facts they will find out, or what vulnerabilities they will observe correctly (or incorrectly come to believe in).

Hence, the model developed here treats the probabilities that terrorists will make various possible decisions as parameters whose values are exogenous to the model (though the history of those groups known to have pursued nuclear weapons can offer some limited

---

[5] This summary of the approach is based on Garrick, "Perspectives on the Use of Risk Assessment to Address Terrorism."

[6] Garcia, *The Design and Evaluation of Physical Protection Systems.*

insight as to what the values of these parameters should be, as discussed in this chapter). Previous attempts to present mathematical models of the dangers of nuclear terrorism have generally been even more simplistic in their treatment of terrorist decisions, assuming either that the probability of a nuclear theft attempt simply scales linearly with either the quantity of material[7] or the number of facilities from which material could be stolen.[8]

I have emphasized keeping the model simple, as a tool for understanding and discussion. Because so little is known about the values of the different parameters that affect the risk of nuclear terrorism, increasing the sophistication of the model would make it harder to understand and use without increasing its fidelity in reproducing the characteristics of the problem. Similarly, because the uncertainties are so large – and even the shape of the distributions of the individual parameters is entirely unknown – I have not attempted to model the uncertainties formally using Monte Carlo simulation or other approaches. Formal modeling of the uncertainty would make the model more complex, yet would require a range of assumptions about parameter distributions that would themselves exaggerate how much is known. (Indeed, formal attempts to model uncertainty often greatly understate the real uncertainty, as uncertainties in parameter values that are formally modeled are often a far less important source of uncertainty than choices concerning the basic intellectual frame and structure of the model.[9]) Instead, in what follows I discuss the uncertainties qualitatively and provide examples of how the results would change with particular changes in key parameters. This model, in short, is one simple first cut, designed to illuminate particular issues about the possible terrorist pathways to the bomb and what might be done to block them; it is by no means a final answer to the problem of modeling nuclear terrorism.

The model presented here focuses on a small number of terrorist groups which have made the decision to attempt to get and use nuclear explosives, and have the resources to give them some non-zero probability of success. Each such group has to decide how much of its efforts and resources to focus on nuclear acquisition attempts versus other activities. When it decides to undertake a nuclear acquisition attempt, it has four pathways to choose from: carrying out or instigating an insider theft at a nuclear facility or transport leg; carrying out or instigating an outsider theft; attempting to buy a nuclear weapon or weapons-usable material from a nuclear black market; or attempting to convince a state to provide a nuclear weapon or weapons-usable material. Each of these pathways offers some probability of success; if it succeeds in getting the material it needs for a bomb, the group then has some probability of succeeding in making a nuclear bomb that would detonate when desired; and it then has some probability of choosing to, and being able to, deliver the bomb to a target location and then detonating it. Each of the groups and its acquisition attempts is assumed to be independent of the others. Figure 3.1 shows the event tree the model is based on, with the early branches based on terrorist decisions to pursue particular pathways, and the later branches based on their success or failure at particular steps on those pathways. In essence, the model simply takes the probability that terrorists will decide to, and manage to, pass each step on this

---

[7] See the simple model presented by Edwin Zebrowski, in *Conversion of Research and Test Reactors*, pp. 60-74.
[8] Avedon, "On the Future of Civilian Plutonium".
[9] Igor Linkov and Dmitriy Burmistrov, "Model Uncertainty and Choices Made by Modelers: Lessons Learned from the International Atomic Energy Agency Model Intercomparisons," *Risk Analysis* 23, no. 6 (2003).

pathway and multiplies them to find an overall estimate of passing through the entire pathway.

This model is intended only to analyze the risk of the actual terrorist use of nuclear explosives: it would need to be modified (in some cases substantially) to be used to analyze other nuclear-related types of terrorism, from radiological "dirty bombs" to sabotage of major nuclear facilities to nuclear hoaxes.

Introducing the Model

The model is driven by the decisions, and the successes and failures, of individual terrorist groups making attempts to get nuclear weapons or the materials to make them. Hence, the first input parameter is the number of groups making such attempts. At any given time, there will be N_n terrorist groups in the world that have decided to attempt nuclear violence and that are capable and sophisticated enough to have some non-zero probability of success (the subscript n denoting nuclear terrorists).[10]

Each year, each particular group j of these N_n groups will have some probability $P_{a(j)}$ of launching a significant attempt to acquire a nuclear weapon or the nuclear materials essential to making one (rather than spending its organizational effort on other activities). $P_{a(j)}$ is quite likely to be different for different groups.

The expected number of acquisition attempts per year, A, is the sum of the probabilities of deciding on such an attempt for all of the groups that might do so:[11]

$$A = \sum_{j=1}^{N_n} P_{a(j)}$$

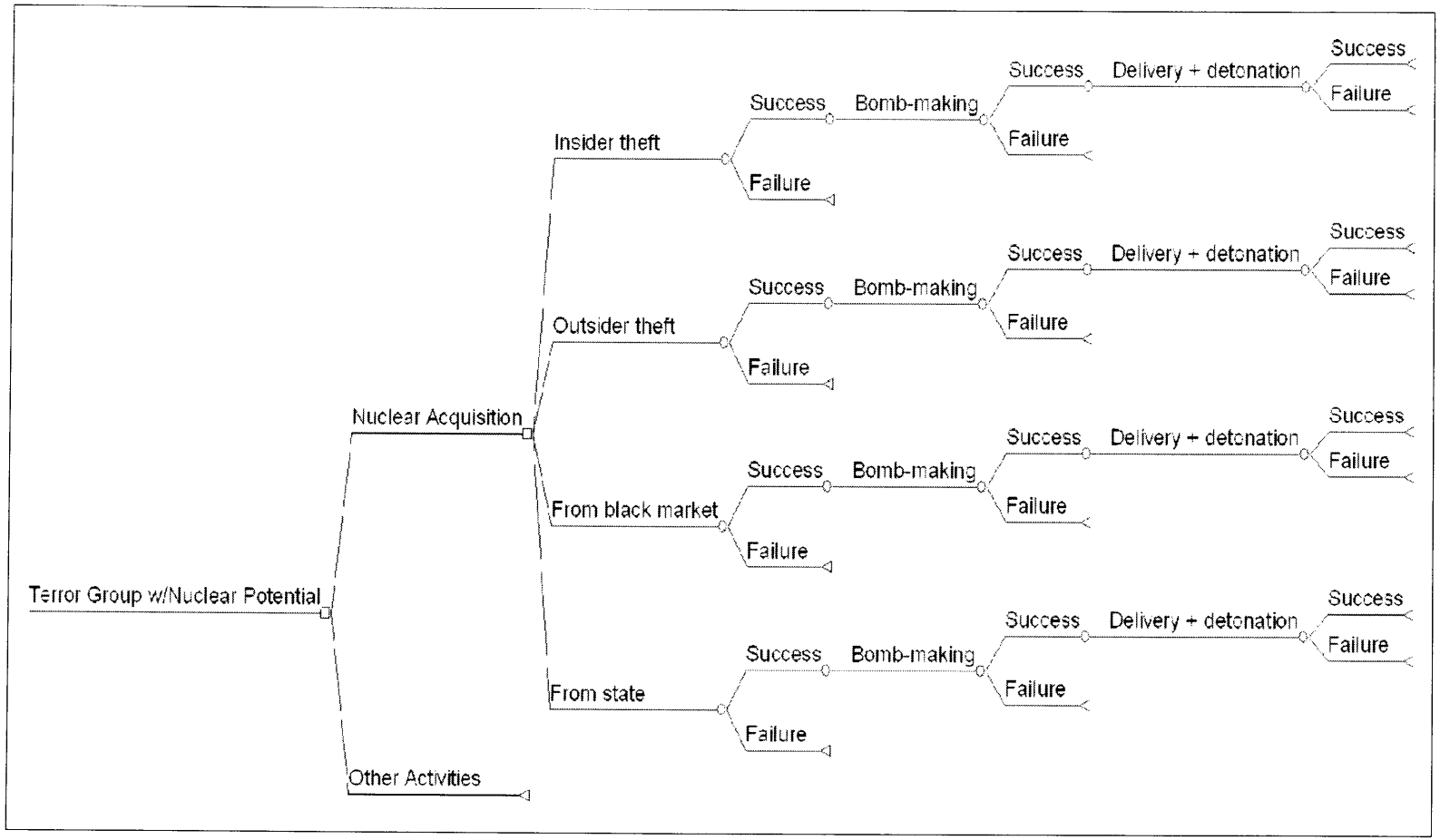
These acquisition attempts will have probability $P_{o(j)}$ of being based on carrying out or instigating an outsider theft attempt at a facility or transportation leg; probability $P_{i(j)}$ of being based on instigating a theft attempt by insiders with authorized access to the facility or transportation leg; probability $P_{b(j)}$ of being based on attempting to purchase such items from others who have stolen them on some kind of nuclear black market; and probability $P_{n(j)}$ of being based on deliberate provision of such items by a nation-state in possession of them.

---

[10] In cases like the loose network of groups that post-9/11 al Qaeda has become, one could model these groups as one group called al Qaeda, or, equivalently, as a large number of separate groups, each with a correspondingly lower yearly probability of launching a significant attempt to acquire a nuclear weapon or the materials to make one. In what follows, al Qaeda is treated as a single group.

[11] This assumes a maximum of one serious acquisition attempt per year per group, adequate for the purposes of this simple model. (If there are several groups, however, there may be several acquisition attempts in one year.) One easy way of relaxing this assumption would be to use a smaller unit of time, such as a month or a week, and adjust estimates of $P_{a(j)}$ accordingly.

Figure 3.1: Nuclear Terrorism Model Event Tree



Acquisition attempts are divided into these categories in the model because the policy prescriptions for reducing the probability of success for each of type of acquisition attempt are different.[12] In this model, these are the only possible paths for an acquisition attempt.

Each acquisition attempt k will have some probability of being successful – $P_{os(j,k)}$, $P_{is(j,k)}$, $P_{bs(j,k)}$, $P_{ns(j,k)}$. These probabilities, too, are likely to vary from one group to the next and from one acquisition attempt by that group to the next.

In the event that an acquisition attempt is successful, there will be some probability $P_{w(j,k)}$ that the group that acquired the items will successfully be able to transform them into a workable nuclear explosive capability that would in fact detonate (including transporting them to the location where the group would work on this transformation, if necessary). Once the group has a usable nuclear capability, there will be some probability $P_{d(j,k)}$ that they will decide to, and be able to, deliver the bomb to its intended target and detonate it.

The probability $P_{s(k)}$ that any given acquisition attempt k will be successful, and will ultimately lead to a terrorist nuclear attack, is given by taking each of the pathways on the event tree and multiplying out the probability of success on that path (including the probability that the terrorists will choose that pathway, the probability that the chosen acquisition attempt will succeed, the probability that the recipients will then be able to make a workable bomb, and the probability that they will be able to, and decide to, detonate that bomb), and then adding up the results for the different pathways:

$$P_{s(k)} = \left(P_{o(j)}P_{os(j,k)} + P_{i(j)}P_{is(j,k)} + P_{b(j)}P_{bs(j,k)} + P_{n(j)}P_{ns(j,k)}\right)\left(P_{w(j,k)}P_{d(j,k)}\right)$$

Hence, the overall probability P_c of a terrorist nuclear catastrophe somewhere in the world in any given year can be found by multiplication of the probabilities from each of the acquisition attempts: [13]

---

[12] In many cases, outsiders and insiders might work together – for example, an insider might tell outsiders about the details of the site's security arrangements and possibly disable some security measures to facilitate an outsider attack. In this simple model, such combined insider and outsider attacks are treated as one subset of insider theft, because two of the most important differences between outsider and insider thefts – the need to convince at least one authorized insider to participate and the possible knowledge of the confidential details of the security system that an insider could bring – apply in such combined cases as they do in cases involving only insiders.

[13] In cases where there are not an integer number of expected acquisition attempts per year, this simplified notation for multiplying from 1 to A is not appropriate; one obvious solution is to integrate the risk over a period of time for which the expected number of acquisition attempts is an integer.

Note here that I am using a linear model of the accumulating number of acquisition attempts, but an exponential model for the risk of an actual terrorist nuclear detonation. An exponential model is appropriate when one occurrence of an event would transform the situation, so that the relevant question is "what is the probability of greater than zero occurrences?" This is certainly the case for a terrorist nuclear attack, as responses to such an event would transform the probabilities of further such attacks. But in assessing the risk posed by events that happen regularly without changing the overall situation, a linear model is most appropriate. For example, if a tall building with a lightning rod has a 50% chance of being struck by lightning each year, and those lightning strikes have no major effect on the building, one would expect that over 10 years there would be an average of 5 lightning strikes. If, on the other hand, a lightning strike would destroy the building, the relevant question is "what is the chance of avoiding having even one lightning strike?" For that question, an exponential

$$P_c = 1 - \prod_{k=1}^{A} \left(1 - P_{s(k)}\right)$$

$$= 1 - \prod_{j=1}^{\sum_{n} P_{a(j)}} \left(1 - \left(P_{o(j)} P_{os(j,k)} + P_{i(j)} P_{is(j,k)} + P_{b(j)} P_{bs(j,k)} + P_{n(j)} P_{ns(j,k)}\right)\left(P_{w(j,k)} P_{d(j,k)}\right)\right)$$

This probability can be converted into the risk of nuclear terrorism, R_c, by multiplying it by the consequences of the event, C_c:

$$R_c = P_c C_c$$

Now the problem boils down to considering the factors that affect the various terms in the equations for P_c and R_c. The many different policy prescriptions that have been offered for dealing with the danger of nuclear terrorism amount, in effect, to different perceptions concerning which of the factors in these equations offer the most promise for risk reduction resulting from government policies.

A Numerical Example

Suppose, as one plausible estimate, that the factors in the equations for P_c and R_c have the following numerical values. For simplicity, assume for the sake of this example that the various probabilities are the same for all groups in the set N_n and for all acquisition attempts of a given type by those groups:

Number of plausible nuclear terrorist groups, N_n=2
Yearly probability of an acquisition attempt by a particular group, $P_{a(j)}$=0.3
Probability of choosing an acquisition attempt based on outsider theft, $P_{o(j)}$=0.2
Probability of choosing an acquisition attempt based on insider theft, $P_{i(j)}$=0.3
Probability of choosing to attempt to purchase black market material, $P_{b(j)}$=0.3
Probability of choosing to attempt to convince a state to provide material, $P_{s(j)}$=0.2
Probability that an outsider theft attempt will succeed, $P_{os(j,k)}$=0.2
Probability that an insider theft attempt will succeed, $P_{is(j,k)}$=0.3
Probability that a black-market acquisition attempt will succeed, $P_{bs(j,k)}$=0.2
Probability that an acquisition attempt from a state will succeed, $P_{ss(j,k)}$=0.05
Probability of being able to convert acquired items to nuclear capability, $P_{w(j,k)}$=0.4
Probability of delivering and detonating bomb once acquired, $P_{d(j,k)}$=0.7
Consequence of terrorist nuclear attack, C_c=$4 trillion

---

model is appropriate, and the answer in this hypothetical case is that the building has only one chance in a thousand of surviving for ten years. The linear model for acquisition attempts used here is probably not strictly accurate, as acquisition attempts that were successful and were detected – especially an overt, violent assault on a nuclear facility or transport to steal nuclear weapons or weapons-usable nuclear material – would themselves provoke reactions that would change the picture significantly. This is discussed in the section "Dynamics of the System," below. I am grateful to Richard de Neufville for encouraging me to be more explicit about the circumstances under which linear and exponential risk models were appropriate.

In this example, the number of plausible nuclear terrorist groups in the world is small but not zero. Each of them has about a one-third chance per year of undertaking a significant nuclear acquisition effort. The chances that the group will decide to base such an effort on organizing an outsider attack on a facility or transportation leg, or on getting a nuclear weapon or materials provided by a state, are each 20%, while the chance that the group will decide instead on attempting to instigate an insider theft or to get material from a nuclear black market are each about 30%. The chance of success is about 20% for an outsider attack or a black-market purchase attempt (meaning that four out of five of such attempts will fail), 30% for an insider theft, and only 5% for an attempt to convince a state to provide a nuclear weapon or the materials to make one.[14] Once the relevant materials have been acquired, the group would have a 40% chance – substantial, though still noticeably smaller than the probability of failure – of succeeding in turning them into a usable nuclear capability that would detonate when commanded to do so without being interrupted (based on the notion that a group determined and sophisticated enough to succeed in getting a nuclear weapon or material would likely be sophisticated enough to acquire the capabilities to turn such material into a bomb and the activities involved in doing so could be difficult to detect and stop). Once the group had a usable bomb, it would have, in this example, a very high probability (70%) of deciding to use it and being able to deliver it to a chosen target.

The consequences figure is intended to include both the immediate destruction caused by a terrorist nuclear blast (estimated in one study to be in the range of $1 trillion for a 10-kiloton blast at Grand Central Station on a typical workday),[15] and at least a portion of the knock-on economic and political effects in the target country and worldwide (which UN Secretary-General Kofi Annan has estimated would be sufficiently severe to push "tens of millions of people into dire poverty," creating "a second death toll throughout the developing world.")[16]

---

[14] The terrorists might choose to try to get a nuclear weapon or the material needed to make one from a state 20% of the time, even if this tactic was much less likely to be successful than other tactics, either because the level of effort required for such an acquisition attempt was less (only inexpensive negotiations rather than expensive logistical and recruitment efforts) or because the terrorists misjudged how promising this acquisition strategy was. In general, *if* one assumes that (a) terrorists are good at judging the relative promise of different acquisition strategies and (b) all acquisition strategies have similar risks and costs for the terrorists, then one would expect that the low-probability-of-success strategies would also have low probabilities that the terrorists would choose them. In general, it would be rational for the terrorists to allocate their effort to different acquisition strategies up to the point where the ratio of the marginal increase in the chance of success with additional effort over the marginal cost and risk of additional effort was equal for each of the strategies.

[15] Matthew Bunn, Anthony Wier, and John Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/cnwm.pdf as of 2 January 2007), pp. 15-19.

[16] Kofi Annan, "A Global Strategy for Fighting Terrorism: Keynote Address to the Closing Plenary," in *The International Summit on Democracy, Terrorism and Security* (Madrid: Club de Madrid, 2005; available at http://english.safe-democracy.org/keynotes/a-global-strategy-for-fighting-terrorism.html as of 10 March 2005).

With these values, one would expect a significant acquisition attempt roughly once every other year:

$$A = \sum_{j=1}^{2} 0.3 = 0.6$$

The probability that such an acquisition attempt would be successful and would lead to the detonation of a terrorist nuclear bomb somewhere in the world would be in the range of 5%:

$$P_{s(k)} = (0.2 \times 0.2 + 0.3 \times 0.3 + 0.3 \times 0.2 + 0.2 \times 0.05)(0.4 \times 0.7) = 0.056$$

Over 10 years, there would be 6 expected acquisition attempts, and the probability of nuclear terrorism over a ten-year period, $P_{c(10)}$, would be just under 30 percent:

$$P_{c(10)} = 1 - \prod_{k=1}^{6} (1 - .056) = 1 - (1 - .056)^6 = 0.29$$

The yearly probability of nuclear terrorism would be just over 3 percent. Multiplying the 10-year probability of nuclear terrorism by the $4 trillion consequences estimate, the overall risk, or expected cost, of nuclear terrorism per decade would be $1.17 trillion (without discounting),[17] or well over $100 billion per year.[18]

The expected losses, *E(L),* resulting from a successful theft of a nuclear weapon or enough nuclear material for a bomb (which can also be thought of as the expected value of preventing such an event) would be over a trillion dollars, in this example, given the significant chance that such a theft would lead to actual nuclear terrorism:

$$E(L) = P_{w(j,k)} P_{d(j,k)} C_c = 0.4 \times 0.7 \times \$4 \times 10^{12} = \$1.12 \times 10^{12}$$

Thus, assumptions similar to these would support estimates of a 30-50% probability of nuclear terrorism over the next decade that have been made by some analysts. (By chance, the 29% over 10 years estimate in this numerical example is identical to the average estimate of the probability of a nuclear attack anywhere in the world over the next ten years in a poll of selected international security experts by Senator Richard Lugar in 2005.)[19] They would also support arguments that if policy options are available that could significantly reduce this risk,

---

[17] The effect of discounting over a ten-year period would be less than the uncertainty in the consequences estimate, and discounting would require determining the appropriate approach for discounting catastrophic loss of life in future years, which is a matter of considerable debate.

[18] Because of the use of an exponential model, one cannot simply divide the 10-year expected cost by ten. The yearly expected probability of nuclear terrorism in this example is 0.34%, for an expected yearly cost in the range of $130-$140 billion.

[19] See Richard G. Lugar, *The Lugar Survey on Proliferation Threats and Responses* (Washington, D.C.: Office of Senator Lugar, 2005; available at http://lugar.senate.gov/reports/NPSurvey.pdf as of 2 January 2007). While this was the estimated probability for any type of nuclear attack, whether by a terrorist or by a state, 79% of respondents judged that a terrorist use of nuclear weapons was more likely than state use over the coming decade.

it would be worth spending large amounts of money and political capital to implement those policies.[20]

Those who disagree with one or more of the parameter estimates used in this example (which are discussed in more detail below) can plug alternative figures into the model to examine what their impact would be; the value of the model is not dependent on accepting the particular estimates used in this example. If, for example, the probability of success in turning the stolen items into a usable nuclear capability and the probability of success for each of the types of acquisition attempt were both half the figures used here – perhaps because successful policies had managed to reduce them – then the yearly probability of nuclear terrorism would be 0.8% and the 10-year probability would be 8%. A probability of 1% over 10 years, suggested by some analysts, would require reducing these factors even further, or reducing the yearly probability of an acquisition attempt (because the groups judged the prospects of success to be so poor that they focused their efforts in more promising areas). Even with only a 1% probability over ten years, the expected cost per decade would be $40 billion (without discounting), or $4 billion per year.

Assessing Each of the Factors – and Policies to Influence Them

The Number of Plausible Nuclear Terrorist Groups, N_n

The number of terrorist groups interested in getting and using nuclear weapons and with enough capability to have some chance of success in doing so is likely to be small. A reasonably strong case can be made that this number was zero for essentially all of the period from the invention of nuclear weapons to the late 1980s (when both Aum Shinrikyo and al Qaeda began to take shape). Today, as discussed in Chapter 2, it appears that N_n is in the range of one to two; that is, this category may include al Qaeda (with some of its derivatives),[21] and possibly also some subsets of Chechen terrorists). While the U.S. Director of National Intelligence has recently estimated that "nearly 40 terrorist groups, insurgencies, or cults have used, possessed, or expressed an interest in chemical, biological, radiological, or

---

[20] For a discussion using similar economic-based reasoning to come to the same conclusion, see Matthew C. Weinzierl, "The Cost of Living: The Economics of Preventing Nuclear Terrorism," *The National Interest*, no. 75 (Spring 2004; available at http://www.findarticles.com/p/articles/mi_m2751/is_75/ai_n6076390/pg_1 as of 22 May 2006), pp. 118-122.

[21] Although the central al Qaeda organization has been heavily damaged since 9/11, in its ambitions and remaining capabilities, it is a more plausible candidate for nuclear terrorism than the many small jihadi groups it has inspired. Nevertheless, given the relatively modest total resources that might be required to make a crude bomb if a terrorist group got the necessary nuclear material, no one can rule out entirely the possibility that some currently unknown jihadi group might be able to commit an act of nuclear terrorism. In this simple model, al Qaeda could be treated as one entity, or, perhaps more realistically, the central organization and some of the more capable jihadi groups might be treated separately; this would increase N_n, but since the chance of success of the more minor groups would be very small, it would not drastically increase the overall estimated risk.

nuclear agents or weapons," the reality is that only a small fraction of these would have any hope of getting and using a nuclear explosive capability.[22]

N_n is presumably affected by (a) the state of the wide range of grievances and other factors that motivate large-scale terrorism; (b) the personal and organizational characteristics and evolution of particular terrorist leaders and groups; (c) the effectiveness of counterterrorist efforts, particularly those targeted on identifying and disrupting those groups with ambitions and capabilities that make nuclear terrorism a plausible possibility; and (d) perceptions, among terrorist groups interested in causing (or threatening to cause) large-scale destruction, of the utility for their purposes of nuclear explosives compared to other weapons, and of the difficulty of getting and using a nuclear explosive compared to the difficulties of getting and using other types of weapons. The more that terrorists conclude that they are more likely to succeed in accomplishing their objectives by means other than the use of nuclear explosives, the fewer groups are likely to be seriously pursuing nuclear terrorism.

Most policy recommendations to reduce N_n focus on either addressing the root causes of large-scale terrorism or improving the targeting and effectiveness of counterterrorist efforts. Others focus on deterring terrorists from seeking nuclear weapons, both by emphasizing the likelihood of the utter destruction of any group that carried out such an attack and all of its sponsors and by emphasizing how difficult acquiring nuclear weapons would be.[23]

To use the model above to assess the effectiveness of these various types of efforts to reduce N_n, one could introduce the factors F_g (the fraction of terrorist groups that would otherwise have been in N_n who do not enter that group because of successes in addressing relevant grievances and other root causes of terrorism); F_l, the fraction of terrorist groups that would otherwise have been in N_n but have been destroyed (or had their effectiveness sufficiently reduced that they are no longer members of N_n) by law enforcement or other counterterrorist efforts; and F_d (the fraction of terrorist groups that are deterred from pursuing nuclear weapons because they do not believe their utility for their purposes and chances of success in acquiring them are high enough to justify the effort involved).

This approach, however, might understate the potential effectiveness of these policy approaches by focusing only on their chance of removing groups from the N_n set entirely, without adding their possible effect on reducing the effectiveness of the groups that remain. Successfully addressing many of the root causes of terrorism, for example, might still leave men like Osama bin Laden and Ayman al-Zawahiri seeking a nuclear capability, but with

---

[22] John D. Negroponte, "Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence" (Washington, D.C.: 2 February 2006; available at http://www.fas.org/irp/congress/2006_hr/020206negroponte.pdf as of 26 December 2006).

[23] Indeed, analysts of nuclear terrorism in the public debate have to constantly balance providing enough public information about the real danger of nuclear terrorism to motivate democracies to act to reduce the danger against providing information that might convince more terrorists that acquiring nuclear weapons was a plausible option to pursue (thereby potentially increasing N_n), or giving them useful information about how to do so; publications such as this one are written with the intention of contributing to reducing the overall risk by helping to motivate effective government action, but have to be cognizant of the danger that going too far could instead increase the risk.

much less chance of success because of greater difficulty in recruiting the relevant people, raising the necessary funds, and the like; counterterrorist efforts, similarly, might substantially reduce the probability that such groups would be able to mount a successful effort to gain and use a nuclear explosive capability without being interrupted in the process. This potential effect could be taken into account by introducing factors P_g and P_l (for the effect on the terrorists' probability of success from addressing root causes and from improved counterterrorist efforts, respectively), which $P_{s(k)}$ would be multiplied by to find a new terrorist probability of success.

If, for example, one uses the values in the numerical example above and considers a proposed increase in counterterrorist efforts that might result in F_l=0.2 (that is, 20% of the groups previously in N_n would be removed from the category) and P_l=0.6 (that is, the remaining groups' probability of success would be reduced by 40%), then:

$$N_n = 2 \times 0.8 = 1.6$$

$$P_{s(k)} = 0.056 \times 0.6 = .034$$

These groups would then be expected to carry out an average of 0.48 acquisition attempts per year, or 4.8 attempts over 10 years:[24]

$$P_{c(10)} = 1-(1-.034)^{4.8} = .15$$

In other words, although the hypothetical increased counterterrorist effort in this example was only modestly successful, the effort would cut the ten-year probability of nuclear terrorism in half, from 29 to 15 percent.

To reduce the uncertainty in estimating the parameter N_n, it would be important to collect information, to the extent possible, on:

- Particular terrorist groups' focus, or lack of focus, on inflicting mass destruction (and ideologies that might lead to such a focus, such as Aum Shinrikyo's ideas related to its role in a coming Armageddon-like crisis);
- These groups' specific statements and actions related to nuclear matters (and in particular their perception of the utility of acquisition and use of nuclear weapons, and attempts to acquire nuclear capabilities, if any can be identified); and
- These groups' resources and organizational and technical capabilities, as they relate to a potential effort to get and use a nuclear bomb.

The Yearly Probability of an Acquisition Attempt, $P_{a(j)}$

The probability that a group seeking nuclear weapons will launch a significant acquisition effort in any given year is difficult to assess. While a case could be made that such efforts may be more continuous, using various potential strategies, than discrete decisions to make an attempt using a specific strategy, any serious effort to organize an

[24] In reality, of course, an acquisition attempt either occurs or it does not; while there will always be an integer number of real acquisition attempts over any given period, there can be a non-integer expected number of acquisition attempts, and the mathematics works as well with non-integer numbers.

outsider attack on a facility, or to instigate an insider theft at a facility, would require a series of definite decisions involving choosing a target, organizing or recruiting personnel for the attempt, planning the attempt, and so on. Hence modeling these strategies as the products of a definite decision to make a significant acquisition attempt in a particular year makes sense.

Even in the case of purchasing "loose" material from a black market, where one could argue that for a group interested in such material the search is always underway, a case can be made that the decision to pursue a significant acquisition attempt arises when either (a) the group decides to send an agent out in search of such material, or (b) the group decides to take seriously a purchase proposed by a black market participant. In the case of acquisition from a state, the decision may be initiated by the state rather than by the group, but the probabilities will work in much the same way – and in any case, if a state proposes a transfer, the group still has to make a decision as to whether to pursue discussions of the idea seriously.

The history of known acquisition attempts is discussed in more detail below, with respect to each of the types of acquisition attempt; but it is clear that the known number of cases is small, in the range of 3-6 over the last fifteen years. If the known cases represented the total number of actual cases and one concluded that for most of that period N_n=2, then a reasonable estimate of $P_{a(j)}$ for the nuclear terrorist groups observed in recent times would be 10-20% per year. If, on the other hand, a substantial number of acquisition attempts took place that were never detected, then the figure might be higher, in the range of 30-40% per year, as in the numerical example above.

$P_{a(j)}$ is presumably influenced substantially by the group's assessment of the probability of success – that is, many groups are likely to behave somewhat opportunistically, launching an acquisition attempt when they think they see a good chance of getting a nuclear weapon or nuclear material. In general, the terrorists' decisions about whether to attempt to get a nuclear weapon (or the material to make one) or to put their efforts into non-nuclear types of attacks will be made in an ongoing strategic game with governments deciding how to invest (or require the private sector to invest) in preventing and protecting against the most devastating types of attacks.[25] If government actions to prevent nuclear terrorism are seen by terrorists in the N_n group as sufficient to make the probability of successful terrorist acquisition of a usable nuclear explosive capability very low, the terrorists would presumably turn their attention to other potential avenues of attack.[26] Hence, policy measures to reduce

[25] For a discussion of the application of game theory to modeling this terrorist decision-making, see, for example, Woo, "Quantitative Terrorism Risk Assessment." For a useful mathematical model and discussion of terrorist choices in allocating their resources, as they relate to choices by the potential targets to invest in varying levels of protection, see Darius Lakdawalla and George Zanjanji, *Insurance, Self-Protection, and Economics of Terrorism* (RAND Center for Terrorism and Risk Management Policy, 2004; available at http://www.rand.org/pubs/working_papers/2005/RAND_WR171.pdf as of 11 February 2006).

[26] As one might expect, game theory analyses of this interaction suggest that it is rational to invest most in protecting those facilities where a successful terrorist strike would have the highest consequences (a category that certainly includes facilities where nuclear weapons or their essential ingredients could be stolen). If such facilities *are* provided with high levels of protection – which is not yet universally the case, as discussed in the previous chapter – terrorists may maximize their utility by attacking less defended, but lower-consequence, targets. In the simple model used here, no assumption is made that governments have yet been rational enough to put in high levels of security at every high-consequence location. Nor is any assumption made that terrorists

the chance of a successful acquisition – and to reduce terrorists' perception of that chance – would presumably reduce $P_{a(j)}$ for most groups.

To reduce the uncertainty in estimating the parameter $P_{a(j)}$, it would be important to collect information, to the extent possible, on all past nuclear acquisition attempts by terrorist groups, as well as on the extent to which any of the past cases of nuclear theft and smuggling appear to have involved a specific buyer attempting to get the stolen items.

The Probabilities of Outsider Theft Attempts, $P_{o(j)}$ and $P_{os(j,k)}$

Terrorists will presumably choose the means to get nuclear material they think is most likely to work. Hence the probability that a particular group will choose to undertake an acquisition attempt based on an outsider theft, $P_{o(j)}$, will presumably be closely related to their perception of $P_{os(j,k)}$, the probability that an outsider theft attempt would succeed.

$P_{o(j)}$ appears to be small: there are no confirmed incidents in the historical record of outsider attacks on nuclear facilities or transports that were instigated by terrorists and were clearly intended for the purpose of stealing nuclear weapons or materials. This is something of a puzzle, since, as described in Chapter 2, some nuclear facilities around the world – particularly research reactors fueled with highly enriched uranium (HEU), a potential nuclear bomb material – have no more than a night watchman and a chain-link fence for their security, arrangements that could readily be defeated by attack capabilities terrorists have demonstrated in other contexts, suggesting that for some facilities, $P_{os(j,k)}$ may be quite high. Several plausible explanations of this puzzle suggest themselves. Terrorists may have limited information about nuclear matters, including which sites have weapons-usable nuclear material and what their security arrangements are; they may believe (perhaps correctly) that nuclear theft by open frontal assault would lead to such an intense government response attempting to find and recover the stolen items that their chances of successfully turning them into a usable nuclear explosive capability would be substantially reduced;[27] or they may have felt that they were not yet sufficiently prepared to make a bomb to pursue a theft option that would openly announce their intentions.

Over the years, however, there have been a number of incidents, from terrorists attacking a U.S. nuclear weapons base in Germany in 1977 to terrorist teams carrying out reconnaissance at Russian nuclear warhead storage facilities in 2001, which collectively suggest that $P_{o(j)}$ is not zero.[28] There have also been documented cases of outsider thefts of

---

are always rational in their choices of where to allocate their effort; as noted earlier, available evidence concerning the nuclear programs of Aum Shinrikyo and al Qaeda suggests that this is not the case.

[27] For one discussion of some of the difficulties thieves might face after such an overt assault, see William Langewiesche, "How to Get a Nuclear Bomb," *Atlantic Monthly* 298, no. 5 (December 2006), pp. 80-98. Unfortunately, that account grossly overstates the difficulties the assailants would face in melting away after such an assault, and essentially rules out such assaults as realistic possibilities. In a large number of cases in Russia, by contrast, Chechens have assaulted targets in force and then escaped without being caught.

[28] A detailed publicly available account of the 1977 incident, making the case that it was an attempt to steal nuclear weapons, can be found in Andrew Cockburn and Leslie Cockburn, *One-Point Safe* (New York: Anchor Books/Doubleday, 1997). The base commander at the time, however, believes that it was merely an attack on the base, not an attempt to steal nuclear weapons; if that had been the purpose, in his view, the terrorists would

nuclear material not instigated by terrorists – though in the known cases these outsiders had help from insiders, a situation that would be classified as an insider theft in the simple model used here.[29]

Of course, overt frontal assaults are not the only options available for outsider theft attempts: covert outsider thefts, such as efforts to tunnel into a vault from outside (a tactic used successfully in a number of recent bank robberies around the world),[30] or thefts based on deception (such as using forged identifications, uniforms, and authorization papers to convince staff that the thieves are authorized to remove nuclear material for transport to another site)[31] are also possibilities which must be guarded against.

The Design Basis Threat and Conditional Risk

Currently, the most commonly used approach to assessing the probability of successful outsider or insider theft from a particular nuclear facility or transport leg is the use of vulnerability assessments based on a specific set of potential adversary capabilities against which the facility is required to be able to defend, the (DBT). A vulnerability assessment is intended to assess the probability that the security system could defeat an adversary with the

---

have brought a larger and more capable force for the job. (Interview with Maj. Gen. William Burns (U.S. Army, Ret.), August 2002.) For the 2001 incidents, see "Russia: Terror Groups Scoped Nuke Site," *Associated Press*, 25 October 2001; Pavel Koryashkin, "Russian Nuclear Ammunition Depots Well Protected – Official," *ITAR-TASS*, 25 October 2001. There have been a substantial number of other terrorist incidents involving nuclear facilities over the years – including one in which a group of armed terrorists overwhelmed the guards and took complete control of a nuclear facility under construction – but these other incidents do not appear to have been carried out with nuclear theft in mind. For a listing of such incidents through the mid-1980s, see Konrad Kellen, "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists," in *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Cambridge, Mass.: Lexington Books for the Nuclear Control Institute, 1987).

[29] For a detailed account of one remarkable case of this kind, in which the Russian military prosecutor concluded that "potatoes were guarded better" than the stolen nuclear material, see Oleg Bukharin and William Potter, "Potatoes Were Guarded Better," *Bulletin of the Atomic Scientists* 51, no. 3 (May-June 1995), pp. 46-50.

[30] For a description of one recent case involving a tunnel into a bank vault, resulting in the theft of tens of millions of dollars, see Stan Lehman, "In Brazil: Thieves Tunnel into Bank Vault for $67.8 Million," *Associated Press*, 10 August 2005. For another recent case involving outsiders with insider information stealing tens of millions of dollars in gems and succeeding in keeping the theft covert until after it was complete despite some of the most stringent security measures in the world, see Rachel Bell, "Sensational Heists," in *Crime Library* (Court TV, 2005; available at http://www.crimelibrary.com/gangsters_outlaws/outlaws/major_heists/index.html#continue as of 22 December 2005); "The Great Diamond Heist," "PrimeTime Live," *ABC News*, 12 February 2005. In general, terrorists would presumably prefer to stage a covert theft, rather than an overt attempt to shoot their way into a facility or hijack a nuclear transport – because in the case of an overt attack they would have to cope with possible response forces, pursuit, and what would presumably be a massive government effort to find and retrieve the stolen nuclear weapon or weapons-usable nuclear material. Appropriate investments in security and monitoring can make it quite difficult to keep a theft covert, though, as the examples just mentioned demonstrate, sufficiently clever and capable thieves may still be able to carry off a covert theft.

[31] This type of deception is a common terrorist and criminal tactic. In one recent case, for example, Chechen terrorists truck-bombed the government headquarters in Chechnya – using military uniforms and forged passes to pass through multiple checkpoints before reaching their target. For a brief description, see Guy Chazan, "Chechens Turn on Each Other – after Years of Attacking Russians, Local `Collaborators' Are New Foe," *Wall Street Journal*, 30 December 2002.

maximum capabilities included in the DBT and to identify the most vulnerable pathways the adversary might use, where additional investments in security could most reduce the probability of successful theft.[32] In the DOE regulatory system, for example, facilities are required to estimate the probability that their security system would be effective in defeating the specified threat and to take steps to ensure that this probability of successful protection remains above a specified level (related to the types of nuclear weapons or materials available at the site).

In this system, the risk of nuclear theft from any particular facility is given by:

$$R = P_{at}(1-P_E)C$$

where R is the risk, P_{at} is the probability of a theft attempt at that site, $(1-P_E)$ is the probability that such an attempt would be successful (expressed as one minus the probability that the security system would be effective in defeating the threat), and C is the consequence of theft of the particular types of weapons or materials present at that facility.

Given the difficulty of estimating P_{at}, DOE has based its regulations on limiting "conditional risk" – the risk conditioned on assuming that an attack involving adversaries with the capabilities specified in the DBT occurs, that is, that $P_{at}=1$. Until recently, in the DOE system, facilities were required to calculate the conditional risk at their facility, using the following risk equation:

$$R_{cond} = C(1-P_E)$$

where R_{cond} is the conditional risk posed by possible nuclear theft at a particular facility, C is the consequence of theft of the particular types of weapons or materials present at that facility, and P_E is the probability of effectiveness of facility's security system in defeating the specified threat.[33] (C has typically been rated on a scale of 0-1, imposed by DOE regulators, to avoid the difficulties of estimating parameters such as the adversaries' chances of gaining a usable and deliverable nuclear capability from the stolen items and the consequences if they do.[34]) More recently, because of the uncertainties and controversies in explicitly setting consequence rankings for different types of nuclear materials, DOE has reportedly been moving toward a system based solely on keeping the estimated probabilities of failure to defeat the DBT below specified levels (with the different consequences of theft of different types of material reflected in the probabilities of successful protection the regulations require,

---

[32] For discussions, see, for example, Garcia, *The Design and Evaluation of Physical Protection Systems*; Gardner, "Process of System Design and Analysis." For a summary and critique of such approaches, see Bunn, "Systems Approaches to Security".

[33] See, for example, Gardner, "Process of System Design and Analysis.". See also William C. Brundson, "Nuclear Terrorism Risk Reduction: Evaluating the Effectiveness of the Department of Energy's United States/Russian Nuclear Material Protection, Control, and Accounting (MPC&A) Program" (Ph.D. dissertation, Graduate School of International Studies, University of Denver, 2005); Ronald E. Timm, *Security Assessment Report for Plutonium Transport in France* (Paris: Greenpeace International, 2005; available at http://greenpeace.datapps.com/stop-plutonium/en/TimmReportV5.pdf as of 6 December 2005).

[34] The DOE system is the only one the author is aware of that involves an explicit attempt to make estimates of risk for each facility and to base regulation on those risks.

in the DBT to be defended against, and to some extent in the defense strategy the regulations require).[35]

While the DBT approach focuses on a particular level of adversary capability, the reality is that adversary capabilities may cover a broad distribution, which nuclear security planners can only roughly estimate. The DBT concept is a simplification of this complex reality: since no one knows what the likely distribution of terrorist capabilities is, regulators simply pick one particular point on the spectrum (based on threat intelligence and a range of other factors) and require facilities to be able to defend against a threat with that level of capability. For a particular identified DBT, using vulnerability assessment techniques, it is possible to estimate the change in the probability of successful theft resulting from a particular proposed security upgrade – but that may be a different thing from the change in probability given the actual (but unknown and possibly reactive) distribution of terrorist capabilities.[36]

The Distributions of Security Levels and Terrorist Capabilities

To assess the probability of successful outsider or insider theft, it is essential to consider the distribution of weaker and stronger security systems for nuclear stockpiles around the world, and the distribution of potential adversary capabilities these systems must protect against. The risk of successful outsider or insider nuclear theft will in general be dominated by those facilities or transport legs where nuclear weapons or weapons-usable nuclear material exist that the weakest security and face the highest threats – because terrorists and thieves are more likely to choose those points of attack and more likely to succeed if they do.

Since specific nuclear security measures are kept confidential terrorists are likely to have only limited information about them; although they may have better information for judging their own capabilities, they are likely to have limited experience operations comparable to stealing nuclear weapons or weapons-usable materials, so there are likely to be substantial uncertainties in their judgments of what security measures they could realistically defeat, as well. Of course, the information on terrorist capabilities available to nuclear security planners is far more limited – no one really knows how clever a plan, with how many attackers, what weapons, or what capabilities, terrorists might be able to bring to bear to accomplish a nuclear theft.

Nuclear security levels in any particular country are likely to cluster around the measures that country's rules require – but as there are no binding global rules for nuclear security, security levels vary widely from one country to the next, making the global distribution of nuclear security a lumpy sum of national distributions.[37] Figure 3.2 shows a

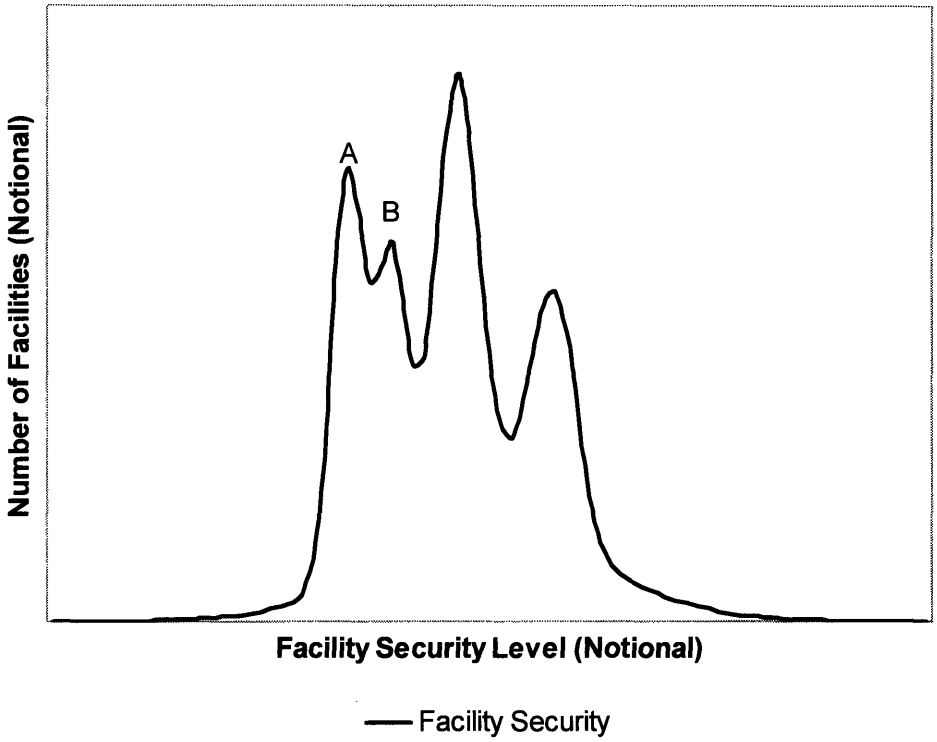
---

[35] Interview with Sandia National Laboratories expert, July 2005.

[36] For a good example of an approach assessing the degree of risk reduction achieved by security upgrades on the basis of changes in the probability that a fixed DBT could carry out a successful theft, see Brundson, "Nuclear Terrorism Risk Reduction".

[37] There are many reasons for these wide variations, based on differences in national culture, varying degrees of concern over the danger of nuclear theft, and the like. In particular, countries that do not believe nuclear terrorism poses a substantial threat to *their* security will have an incentive to invest less in nuclear security;

Figure 3.2: Lumpy Global Distribution of Nuclear Facility Security Levels



notional version of this lumpy global distribution of security levels for nuclear facilities and transport legs throughout the world, with the countries labeled "A" and "B" having the weakest security measures in place.

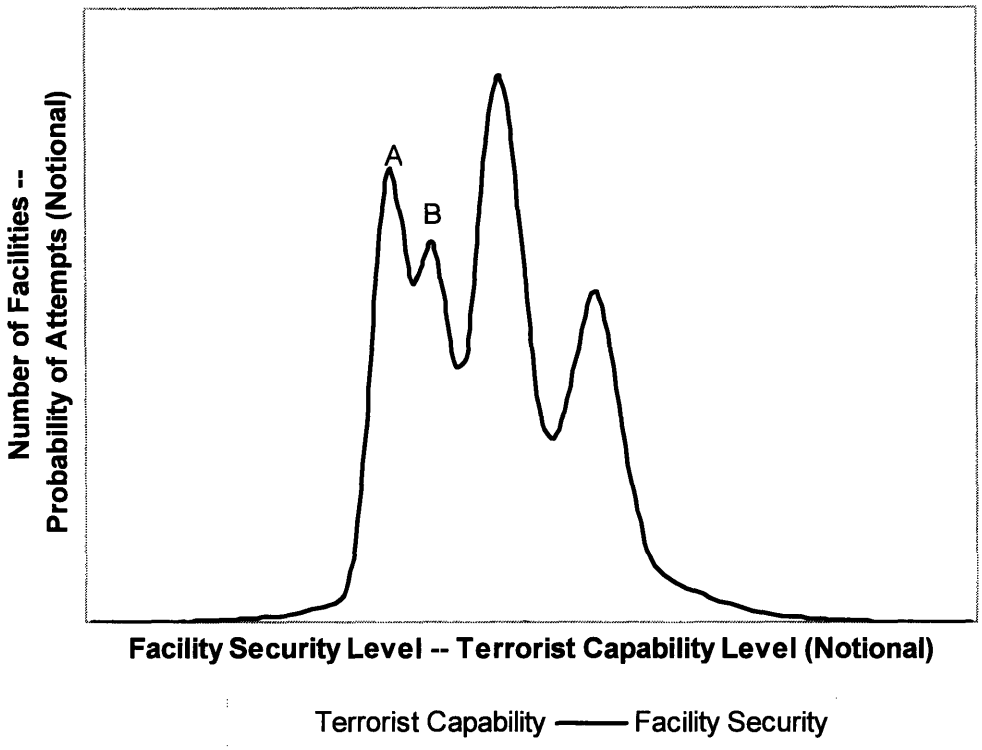
Here, I use "security level" to mean the level of adversary capability that these security systems would have a good chance of defeating. Plotting this on one dimension is itself an abstraction, since different facilities may have security systems that are more or less able to defeat different *types* of adversary capability. One facility, for example, may have skeptical, well-trained personnel better able to defeat a theft attempt based on deception,

---

moreover, there is an "interdependent security" problem, in which countries' incentive to invest in nuclear security is reduced by their perception that much of the threat to their security comes from the possibility of theft in other countries and would not be reduced by investing in nuclear security domestically. See Howard Kunreuther and Geoffrey Heal, "Interdependent Security," *Journal of Risk and Uncertainty* 26, no. 2-3 (2003; available at http://opim.wharton.upenn.edu/risk/downloads/02-06-HK.pdf as of 5 February 2006). To date, however, this effect does not appear to be strong, at least in the U.S. case: although a case can be made that DOE facilities, for example, are already secure enough that very little of the nuclear terrorist threat to the United States comes from theft from U.S. facilities, DOE continues to make substantial investments in upgrading them further (with total annual safeguards and security costs at DOE now well over $1 billion per year).

Even within an individual country, there may be more than one set of rules creating more than one distribution of facility security levels. In the United States, for example, DOE facilities are subject to internal DOE security rules, whose requirements are currently substantially more stringent than those of the Nuclear Regulatory Commission (NRC), which regulates privately owned nuclear facilities.

Figure 3.3: Lumpy Global Distribution of Nuclear Facility Security Levels and the Capability Distribution of One Terrorist Group

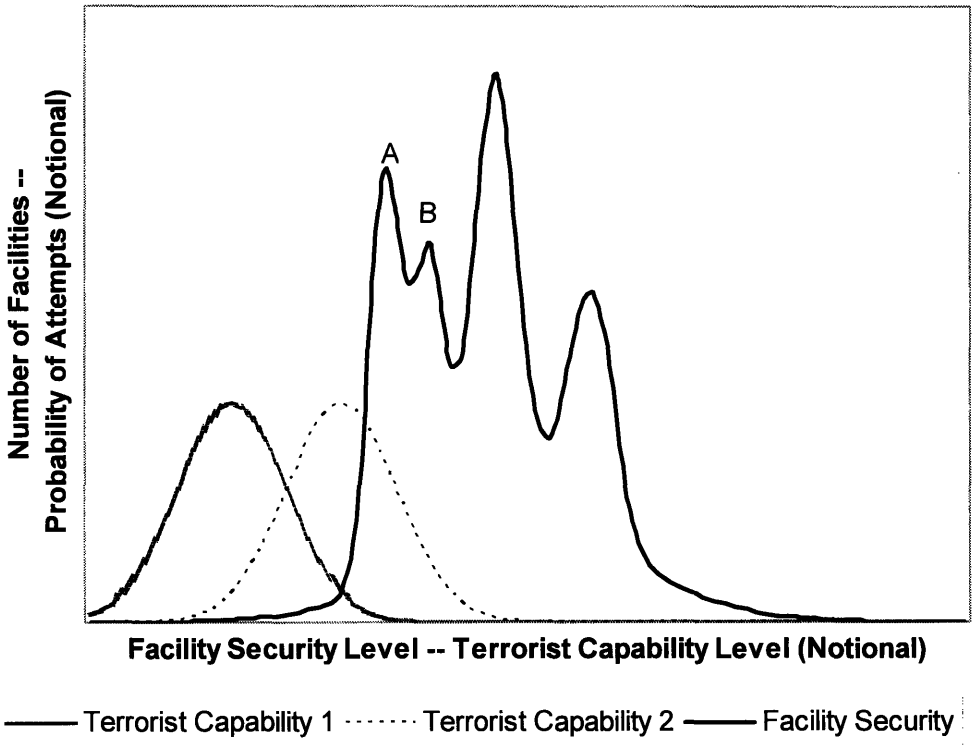


while another may be better protected against an attack using large numbers of attackers, or unusual vehicles.

A terrorist or criminal group considering an attempt to steal nuclear weapons or weapons-usable nuclear material would have an estimate of the capability it could bring to bear for an outsider theft attempt, with some uncertainty. The group would presumably also attempt to develop an estimate – which might or might not be accurate – of how strong the security was at the various facilities where it was considering making its attempt. In the idealized case in which the group had accurate information on security measures worldwide, and was able to bring equal levels of capability to bear anywhere in the world, the situation from the point of view of the group's planners might look roughly like that shown in Figure 3.3. The solid line is the distribution of nuclear security levels, as before; the dotted line represents the terrorist or criminal group's assessment of the level of capability it could bring to bear in a theft attempt, with the associated uncertainty.[38] Only where the distributions of

[38] The group's uncertainty about the capability it would succeed in bringing to bear is portrayed here as completely random (some days they might be lucky, other days less so), and hence following roughly a normal curve. But of course in the real world a large part of the possible uncertainty in the group's estimation of its own capabilities is likely to be systematic; the group may be overly self-confident and overestimate its abilities, or it may not realize how effective whatever combination of deception, violence, stealth, and other tactics it is

Figure 3.4: Lumpy Global Distribution of Nuclear Facility Security With Two Distributions of Adversary Capability



facility security and adversary capability overlapped – that is, where there was some significant probability that the group's capabilities would be enough to beat the security system for a particular nuclear stock – would the chance of a successful outsider theft be significant. For this particular group, with its capabilities, nearly all of the risk of successful nuclear theft comes from the facilities in countries "A" and "B." The overall risk of successful nuclear theft by this group could be reduced dramatically by upgrading security for the facilities in these two countries.

Although al Qaeda and the movement associated with it clearly have some degree of global reach, however, it is clearly not true that they can bring the same levels of capability to bear in every country. The level of capability they could bring to bear in a nuclear theft

---

planning would actually be. The graphs of adversary capability can be interpreted as probability distribution functions whose area sums to one, but the graph of facility security levels, representing a discrete number of nuclear facilities and transport legs, should not be interpreted in that way and has an area much larger than one.

There are many nuclear facilities and transport legs, but only a small number of theft attempts are expected; hence the notional area covered graph of adversary capability is intended as a probability distribution function, and therefore summing to one; the distribution of facility security lev distribution of adversary capability is plotted as a frequency of "attempts" at different levels of capability not because I envision a single group making hundreds of theft attempts, but simply because this might be their assessment of the likelihood that they could bring to bear a given level of capability in a given attempt.

attempt in Pakistan is much higher than the level of capability they could bring to bear in Canada, to take one example. (Means to assess how such threats vary from country to country are discussed in Chapter 4.) Hence, rather than the situation as shown in Figure 3.3, a terrorist or criminal group's planners might face something more like the situation in Figure 3.4. If, for example, the group could only pull together the capability represented by the distribution "Terrorist Capability 1" in Country "A," but could pull together the higher capability represented by the distribution "Terrorist Capability 2" in Country "B," then the probability of a successful theft in Country "B" would be substantially higher even though the facilities in Country "B" are more secure – because there would be far more overlap between the capabilities the group might be able to bring to bear and the capabilities needed to defeat the nuclear security systems in Country "B" and carry out a successful theft. Hence, as discussed in detail in Chapter 4, to assess the risk of nuclear theft posed by different nuclear facilities and transport legs, it is essential to consider not only the strength or weakness of their security arrangements, but also the differing threats that these security arrangements face. Of course, in the real world there are many countries where nuclear weapons or weapons-usable nuclear material are located, not just two, and the terrorist group might have many different levels of capability it could bring to bear in different countries.

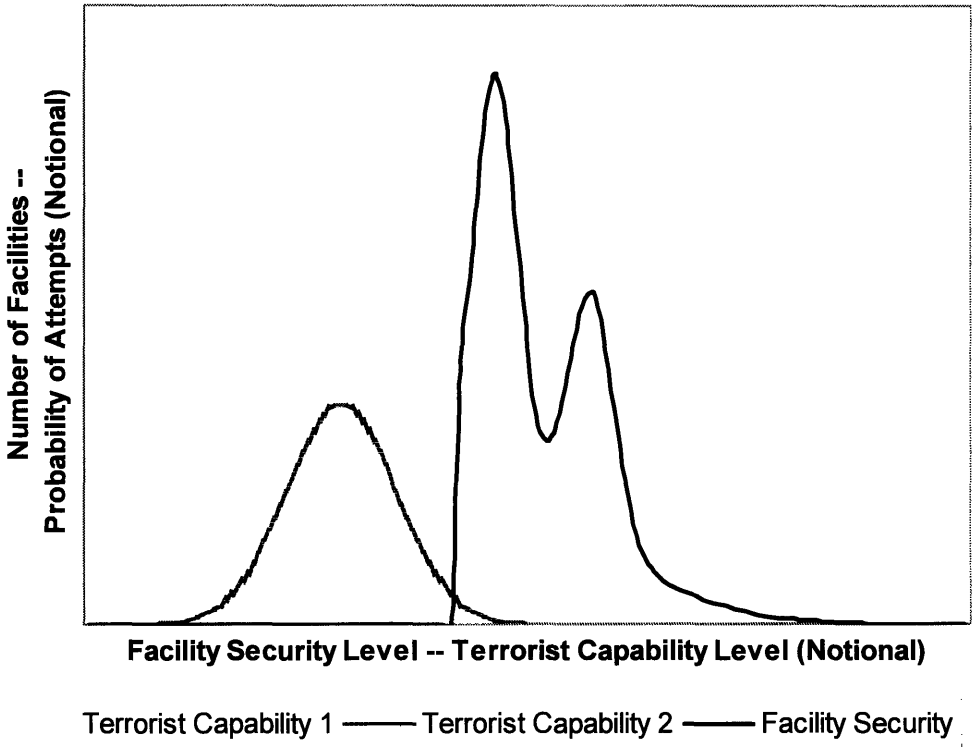
If the two distributions labeled "Terrorist Capability 1" and "Terrorist Capability 2" represented the threats faced by all countries, then the probability of successful outsider theft could be reduced dramatically by upgrading security or removing the nuclear material from the facilities and transport legs in the countries labeled "A" and "B" in that figure. In that case, if one could truncate the lower end of the distribution of security levels – for example by rigorously identifying all the facilities with weaker security and either removing the nuclear material from them or substantially upgrading the security – one might be able to effectively eliminate the portion of the curve which overlaps with the potential adversary capabilities and thus poses a significant risk. See Figure 3.5. This is the rationale for proposals for a "global cleanout" focused on removing all nuclear material from the world's most vulnerable sites as rapidly as possible.[39]

Similarly, if stringent global standards for nuclear security were put in place, the global variation in security levels might be greatly reduced and the mean shifted upward, which could also effectively eliminate the portion of the curve posing a substantial security

---

[39] For one of the early proposals for such a "global cleanout," see Matthew Bunn, John Holdren, and Anthony Wier, *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/securing_nuclear_weapons_and_materials_May2002.pdf as of 2 January 2007). For more recent discussions, see, for example, Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 2 January 2007); Philipp C. Bleek, *Global Cleanout: An Emerging Approach to the Civil Nuclear Material Threat* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2004; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/bleekglobalcleanout.pdf as of 13 April 2005).

Figure 3.5: Truncated Global Distribution of Nuclear Facility Security Levels With Two Distributions of Adversary Capability



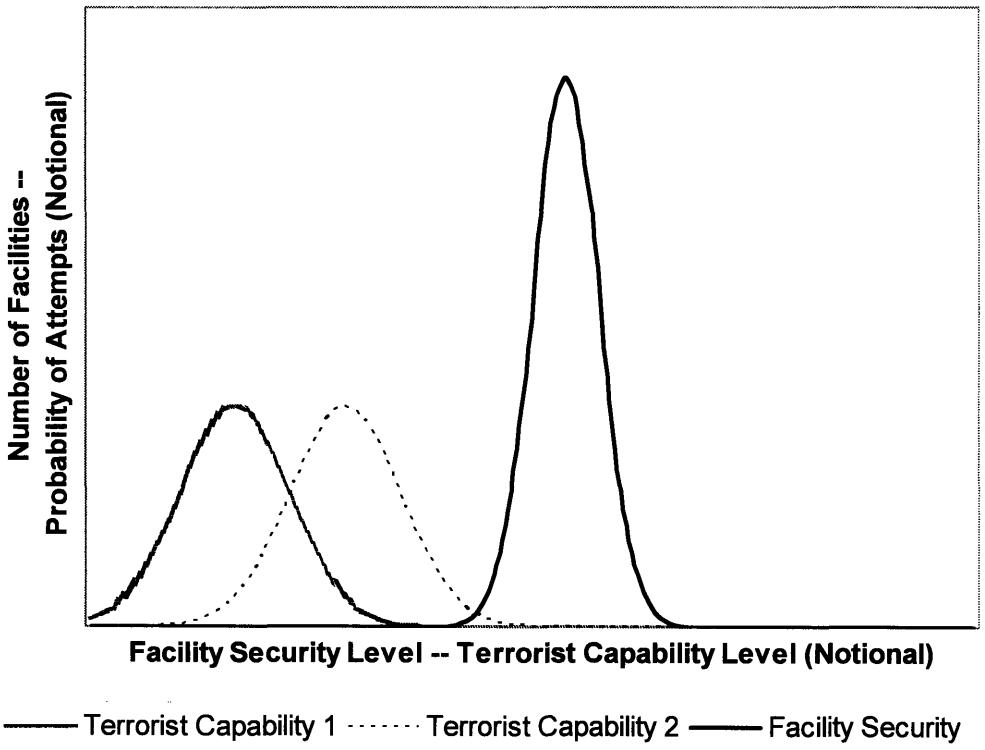
risk.[40] See Figure 3.6. Upgrading security for only some of the vulnerable facilities may not have much benefit in reducing risk, however. If terrorists are able to observe, at least roughly, where facilities have weak security and where they have strong security, upgrading only a portion of the previously vulnerable sites presumably will have the effect of displacing the risk of outsider attack on to other vulnerable sites (just as strengthening security at *all* nuclear sites might have the effect of displacing terrorist efforts onto non-nuclear options).[41]

Two points should be made about this way of conceptualizing the problem, however. First, since nuclear security measures are quite secret, terrorist or criminal groups may be able to collect partial information on the security measures at one or a few sites, but they are hardly likely to have an accurate assessment of security levels at all facilities and transport legs worldwide, as envisioned in Figure 3.3. The uncertainties in their estimates of the

[40] For recent proposals for creating such stringent global standards, see, for example, Bunn and Wier, *Securing the Bomb 2005*; Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004).

[41] For a discussion of the displacement effect from better-protected facilities to less-protected ones, the importance of the observability of protection to that effect, and the effect of increases in average protection of all facilities in increasing the chance that terrorists will turn their attention elsewhere, see the model presented in Lakdawalla and Zanjanji, *Insurance, Self-Protection, and Economics of Terrorism.*

Figure 3.6: Global Distribution of Nuclear Facility Security Levels Meeting Stringent Standards and Two Distributions of Adversary Capability



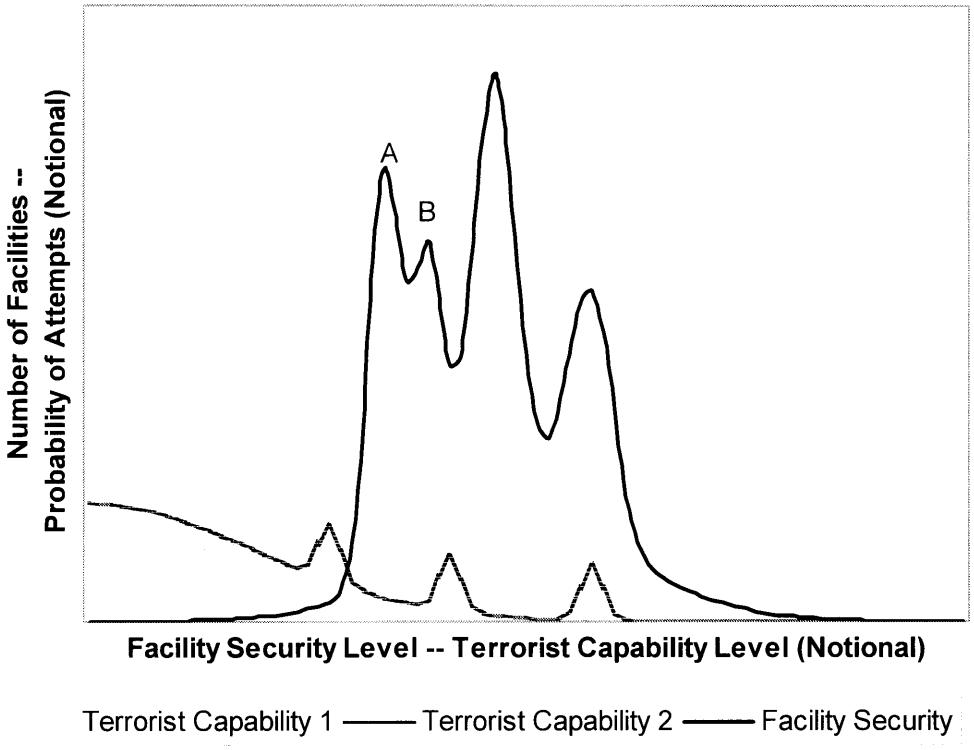
security measures at different facilities – and the resulting probabilities that they may fail to identify the most vulnerable facilities, or may attempt a theft from a facility that has higher security than they expected – clearly reduce the terrorists' probability of success, $P_{os(j,k)}$.[42]

Second, and fundamentally, the picture is likely to look very different from the point of view of those planning defenses against nuclear theft, as opposed to the point of view of the adversary planners. Nuclear security planners would not be dealing with a single terrorist or criminal group with reasonably well-understood capabilities, but with a broad spectrum of possible adversaries whose potential distribution of capabilities was highly uncertain and might include some dangerous outliers with very high levels of capability.

In the case of nuclear security planners considering the entire global picture – such as planners at the IAEA or in a donor state, thinking about where to invest additional resources for security upgrades – the situation might look like that shown in Figure 3.7. In this figure,

[42] Hence, in reality, rather than the two distributions shown in Figure 3.3 , one would have four random variables, each with its own distribution: the real security levels at different sites; the terrorist group's perception of those security levels; the real capability the terrorist group would be able to bring to bear at the moment of the attack; and the terrorists' perception of their capability. Such a situation could be modeled with a Monte Carlo approach, but given that essentially nothing is known about the shapes of any of these distributions, it does not appear likely that such modeling would contribute much additional insight.

Figure 3.7: Lumpy Global Distribution of Nuclear Facility Security With Two Lumpy Distributions of Potential Adversary Capability



"Terrorist Capability 1" represents the uncertain spectrum of potential adversary capabilities that planners might believe a relatively low-threat country faced, while "Terrorist Capability 2" represents the equally uncertain spectrum of capabilities that planners might expect in a higher-threat country. As in Figure 3.3, if the facilities in country "B" faced the higher threat spectrum while facilities in country "A" only faced the lower threat spectrum, the risk of successful nuclear theft would be higher in country "B" than in country "A," with more overlap in the distributions of facility security and adversary capability, even though the facilities in country "B" had somewhat stronger security measures.

It is worth noting that in this figure, the second threat spectrum has one outlier so capable that this group might be able steal nuclear material successfully from all but a few of the most secure nuclear facilities in the world. Estimating just how far out on the curve of adversary capability plausible outliers might be is the fundamental problem for nuclear security planners: they do not want to remain unprotected against threats that have a substantial probability of materializing, but they do not want to waste money attempting to protect against unrealistically capable threats, either. Moreover, they have very little data to go on in estimating what the highest plausible threats in a particular country might be. At a minimum, the types of capabilities that terrorists and thieves have already demonstrated in

that country (or in similar nearby countries) provide a useful guide for the capabilities that nuclear weapons and weapons-usable materials should be protected against.

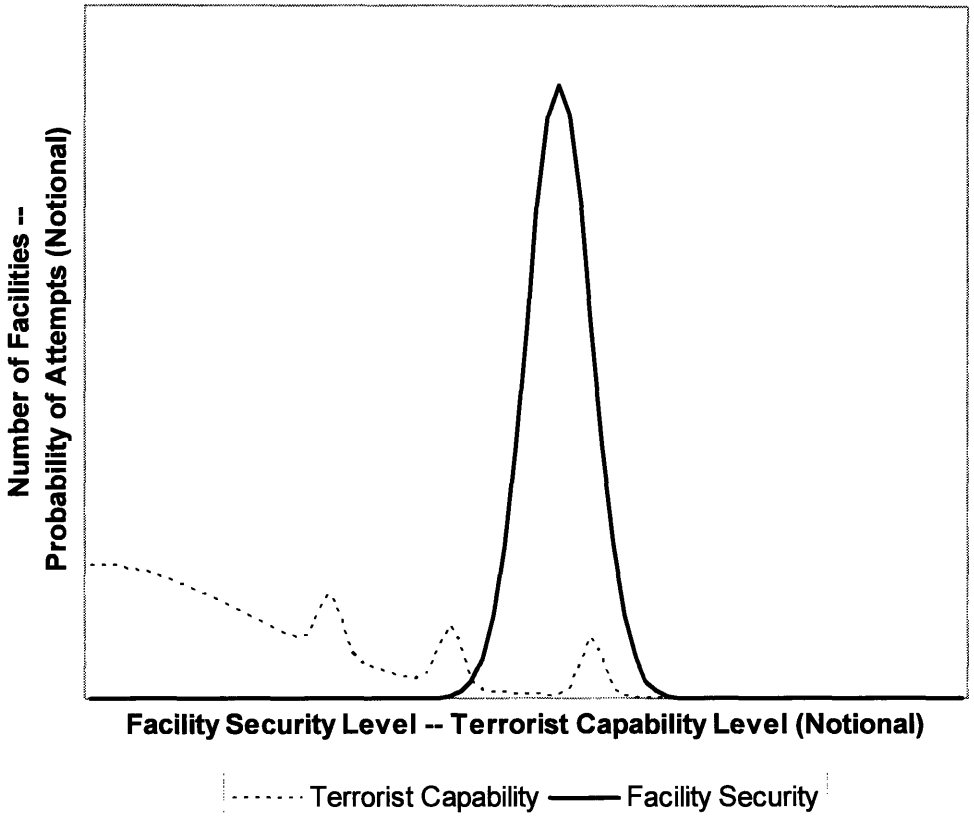
When viewed in this light, measures to remove all the weapons-usable nuclear material from the most vulnerable facilities, or forge stringent global nuclear security standards, as depicted in Figure 3.5 and Figure 3.6, would still have substantial benefit – they would essentially eliminate the risk of successful nuclear theft for all facilities and transport legs facing only the spectrum of adversary capabilities labeled "Terrorist Capability 1," and for those facilities and transport legs facing a spectrum like "Terrorist Capability 2," only the outermost outlier of the adversary capability distribution would remain a substantial concern. But the potential existence of such outliers means that nuclear security planners could have much less confidence in estimating how much the measures they had taken had reduced the risk.

The situation would be somewhat less complicated for nuclear security planners within a single country. They would not be dealing with a lumpy global distribution of facility security levels, but the distribution within their own country, which, as noted earlier, would probably tend to cluster in a distribution around the levels required by that country's nuclear security rules. They would have to estimate only the potential adversary capabilities in their own country, not those that might exist in countries around the world – but they would still face large uncertainties in estimating how far out on spectrum of capability plausible outliers in the distribution of adversary capabilities might be. The situation might appear to them somewhat like that in Figure 3.8. In this figure, the nuclear security rules in this hypothetical country are stringent enough to reduce the probability of a nuclear theft attempt succeeding to a very low level for all of the expected threat distribution except the highest-capability outlier. Such a circumstance might well provoke debate (like the debate that is taken place in the United States in recent years) over how likely a theft attempt at high levels of capability was, and whether it was worth the cost of more stringent security rules that would shift the distribution of security levels further to the right.

The discussion to this point strongly suggests that modest investments in upgrading security for those few facilities where the weakest nuclear security measures face the most substantial threats might drastically reduce the overall probability of successful nuclear theft, by outsiders or by insiders. Two points that might reduce the effectiveness of such modest investments should be kept in mind, however. First, there may be countries where the level of capability that terrorists or criminals can bring to bear is so great that technologies such as stronger fences and better intrusion detectors will not provide effective protection at reasonable cost. If the distribution of adversary capability in Figure 3.8 extended well to the right of that shown, modest investments in additional security would not be enough to substantially reduce the risk of nuclear theft.[43]

[43] By the same token, of course, if the actual spectrum of threats were shifted well to the left of that shown in Figure 3.8, $P_{os(j,k)}$ and $P_{is(j,k)}$ would be close to zero, and no additional investments would be needed; it might be that some of the existing nuclear security investments could be cut back.

Figure 3.8: Distribution of Nuclear Facility Security Levels in One Country With a Lumpy Distribution of Potential Adversary Capability



In both Pakistan and Russia, for example, terrorist attacks have on occasion involved scores of heavily armed terrorists attacking at once, with no warning, and insider conspiracies have occurred that involved several insiders working together. (The threats in both Pakistan and Russia, and what they imply for the risks of nuclear theft in those countries, are discussed in more detail in Chapter 4.) Police and intelligence measures designed to increase the probability that large theft conspiracies would be detected before the theft attempt began are an essential complement to nuclear security measures for nuclear facilities and transport legs themselves; in some cases, investments in improving these police and intelligence measures may be as important in reducing the probability of successful nuclear theft as investments in security measures for particular nuclear facilities or transport legs.

Second, intelligent and adaptive adversaries may react to security upgrades not by giving up, but by increasing their capabilities – recruiting more people, buying better weapons, and developing more sophisticated tactics. If facilities need only defend against a handful of outsiders with limited armament, or one insider, relatively simple and low-cost security upgrades will be sufficient; if, on the other hand, they must defend against multiple teams of numerous, well-trained, and well-armed outsiders and programs to ensure the

reliability of authorized staff are sufficiently weak that conspiracies of 4-5 well-placed insiders are a real possibility, the security measures needed to reduce the risk of theft to a low level would be expensive and complex.

The possibility of terrorists' increasing their capabilities to suit the job they want to do is a key source of the debate over what level of threat nuclear facilities should be required to defend against. Some analysts and regulatory agencies argue that past terrorist attacks have overwhelmingly involved only small numbers of people (or even single individuals) with limited capabilities and that defenses against such limited threats will be sufficient to deal with almost all of the risk. Taking this line of thinking, before 9/11, the U.S. NRC only required U.S. nuclear power plants to be protected against a DBT involving attack by a "small group," reportedly three outsiders, possibly in league with one insider;[44] the DBT for theft of HEU or plutonium was reportedly only modestly higher. Others have argued that typical terrorist assaults involve small numbers of people only because that is what the perpetrators "perceived to be necessary to accomplish their mission," and that such small numbers do "not represent an upper limit on their capacity to mobilize people."[45] Hence, they argue, reducing theft risks substantially is likely to require defending against larger and more sophisticated threats. Incidents worldwide in which terrorists or criminals have demonstrated the ability to attack in large numbers, to use sophisticated weapons and planning, and to recruit or blackmail multiple insiders to participate in theft conspiracies suggest that the threats nuclear weapons and the materials needed to make them should be defended against are substantial (see discussion in Chapter 4).

Terrorists' abilities to increase their capabilities are presumably not infinite, and no one could afford to defend against an infinite threat. But as already discussed, no one knows for sure where the upper bound lies. This uncertainty is leading to a lively debate in several countries concerning what DBT facilities with nuclear weapons or weapons-usable nuclear materials should be required to defend against. By late 2003, for example, in response to the 9/11 attacks, DOE adopted rules requiring its facilities to defend against a significantly more capable DBT than had previously been envisioned – but by late 2004, this new DBT was itself considered inadequate, and a still larger, more capable DBT was adopted, reportedly involving a squad-size attacking force with very capable weapons and tools and sophisticated tactics.[46] Since then, however, there has been mounting criticism of the cost of defending against this new DBT, creating pressure on DOE to reduce the DBT again. Meanwhile, while the NRC has increased the DBT since 9/11, the change has reportedly been relatively modest,

---

[44] See, for example, Daniel Hirsch, "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.thebulletin.org/article.php?art_ofn=jf02hirsch as of 8 January 2007), pp. 38-44.

[45] Brian Michael Jenkins and Joseph L. Krofcheck, "Appendix III-A: The Potential Nuclear Non-State Adversary," in *Nuclear Proliferation and Safeguards* (Washington, D.C.: Office of Technology Assessment, 1977). These authors provide an exceptionally thoughtful discussion of some of the issues discussed in this section.

[46] While the specifics are classified, a useful discussion of how DOE's DBT has evolved since the 9/11 attacks can be found in Project on Government Oversight, *U.S. Nuclear Weapons Complex: Y-12 and Oak Ridge National Laboratory at High Risk* (Washington, D.C.: POGO, 2006; available at http://pogo.org/p/homeland/ho-061001-Y12.html as of 17 November 2006).

so that the DBT that an NRC-licensed facility – even one with tons of HEU metal, the easiest material in the world for terrorists to use to make a nuclear bomb – must defend against is reportedly far less capable than the DBT comparable DOE facilities must defend against.[47] One constraint on terrorists' ability to increase their capabilities is that the probability that law enforcement and intelligence services, mentioned above, will detect and disrupt a conspiracy presumably increases as the size of the conspiracy increases. But incidents from the 9/11 attacks to the Beslan school seizure, where large conspiracies to kill large numbers of people were not detected before the terrorists struck, suggest that only modest reliance can be placed on the assumption that law enforcement and intelligence services will always be able to stop large attacks from occurring.

Examples of the Effect of Security Upgrades in Reducing Risk

In short, if terrorists are constrained from readily increasing their capabilities, investments in improving security or removing nuclear material entirely from those facilities that are most vulnerable and face the highest threats could substantially reduce the probability of a successful outsider theft, $P_{os(j,k)}$. Such investments would therefore in all likelihood also reduce the chance that a terrorist group would choose outsider theft as their route to acquiring nuclear material, $P_{o(j)}$. Counter-terrorist measures, designed to detect and stop any outsider theft plot substantial enough to have a chance of being successful in its early stages, might also reduce $P_{os(j,k)}$, if the ability to collect intelligence on such groups were good enough to have a reasonable probability of uncovering such plotting.

In the numerical example above, of the 29% ten-year total probability of nuclear terrorism, 6.5% was coming from the outsider theft path. If we imagine, a program of security upgrades for the most vulnerable facilities that succeeded in cutting $P_{os(j,k)}$ in half, compared to its value in the numerical example, and reducing $P_{o(j)}$ by 30%, then the probability of outsider theft resulting in successful nuclear terrorism over ten years would be reduced to 2.3%, a nearly three-fold reduction. If the idealized figures in this chapter present anything close to the real situation, it may well be possible, for modest investments, to reduce $P_{os(j)}$ by an even larger factor.

While the specific capabilities and procedures that are most important to defeating outsider theft attempts differ somewhat from those that are most important to defeating insider theft attempts, at most sites where security upgrades are underway, integrated suites of upgrades are being pursued that are intended to reduce both insider and outsider dangers. Removal of nuclear material from vulnerable sites would certainly reduce both dangers.

---

[47] See, for example, discussion in Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, *Nuclear Security: Has the NRC Strengthened Facility Standards since 9/11?* U.S. House of Representatives, 109th Congress, 2nd Session, 4 April 2006 (available at http://reform.house.gov/NSETIR/Hearings/EventSingle.aspx?EventID=41937 as of 6 May 2006); Daniel Hirsch, David Lochbaum, and Edwin Lyman, "The NRC's Dirty Little Secret," *Bulletin of the Atomic Scientists* (May/June 2003; available at http://www.thebulletin.org/article.php?art_ofn=mj03hirsch as of 5 February 2006), pp. 44-51; Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006).

Moreover, security upgrades that simultaneously reduced the probability of success for both outsider and insider thefts would also reduce the probability that a terrorist group seeking nuclear material from a black market would succeed, by reducing the likelihood that others, not directly instigated by the group, would succeed in carrying out insider or outsider thefts so as to make nuclear material available on a black market. In this case, reductions in $P_{os(j,k)}$ would presumably not also reduce $P_{o(j)}$, since all the pathways to acquiring nuclear material other than acquisition from a state would be getting less attractive in tandem; such reductions in the overall chance of orchestrating a theft, however, might well lead to reductions in $P_{a(j)}$, the probability that a particular terrorist group would undertake a serious nuclear acquisition attempt in a given year. In other words, if the terrorist group concluded their chances of getting nuclear material were slim, they might not bother to try, focusing their efforts in other areas instead. If, in the numerical example above, security upgrades managed to cut the probabilities of success for outsider and insider theft in half, and for black-market purchase by 40% (because there is some chance that already-stolen material would be available on a black market), and these reductions led to only a 20% reduction in the yearly probability of a serious acquisition attempt by each group, then the previous 29% 10-year probability of nuclear terrorism would be reduced to 14%:

$$P_{s(k)} = (0.2\times0.2\times0.5 + 0.3\times0.3\times0.5 + 0.3\times0.2\times0.6 + 0.2\times0.05)(0.4\times0.7) = 0.031$$

These groups would then be expected to carry out an average of 0.48 acquisition attempts per year, or 4.8 attempts over 10 years:

$$P_{c(10)} = 1-(1-.031)^{4.8} = .14$$

Effect of Quantity of Material

Once a site has one or a few nuclear weapons, or the nuclear materials to make one or a few nuclear weapons, the danger of outsider theft it poses does not increase much as the stockpile at that site increases. Nuclear terrorists are likely to be focused on getting the ability to detonate one or a few bombs; hundreds are likely to be beyond their reach and their interest. For outsider theft, ten tons of nuclear material are not substantially more difficult to defend than one ton of nuclear material. (Hence, as discussed in more detail in Chapter 4, the common use of total quantities of nuclear material as a rough indicator of the scale of the risk of theft worldwide is not justified.)

Even if a facility has only half or two-thirds of the amount of material required for a bomb, the danger of nuclear theft it poses cannot be dismissed, as incidents such as the 1998 embassy bombings (or the 9/11 hijackings) make clear al Qaeda's ability to strike multiple widely separated targets at the same time. The more thefts that must be successful to get enough material for a bomb, however, the lower the chances will be – so thieves are likely to focus on those locations where one or two thefts would be enough. In other words, the risk that theft of a particular stockpile of nuclear material could lead to terrorists making and detonating a nuclear bomb increases rapidly as the quantity reaches a substantial fraction of the amount the terrorists would likely need for a crude bomb, but then levels off after the

quantity has reached a level sufficient for one or a few bombs (see more detailed discussion in Chapter 4).

Effect of Number of Facilities and Transport Legs

The number of facilities and transport legs that have nuclear weapons or the materials to make them probably does have an important impact on the chances of both outsider and insider thefts. For outsider thefts, with a distribution of security levels at different facilities and transport legs subject to a particular country's rules, increasing the number of facilities and transport legs will increase the chance that a facility or transport leg will exist that is low enough on the tail of this distribution for terrorists to be able to defeat its security system (and that terrorists will be able to identify it as such). For insider theft, more facilities means more groups of people with access to material or knowledge of the security system of a site with such material – and, as with outsider theft, it means more chances that some facility will have security poor enough to cause some one to judge that they could steal nuclear material.

If we imagine, for example, a case in which the security level of the different nuclear facilities and transport legs in a particular country happened to be normally distributed, and the security level at which terrorists would decide to make a theft attempt corresponded to a level two standard deviations below the mean in that country, then if there were five facilities with the relevant materials in the country, the chance of one of them having weak enough security to provoke a theft attempt would be approximately 11%, whereas if there were 10 such facilities in that country the probability would be 21% and with 20 such facilities, the probability would be 37%.[48] (If, on the other hand, the distributions of security and of terrorist capability had enough overlap that it was almost certain there would be a facility that the terrorists could attack, there would not be this strong increase in probability with increasing numbers of facilities. Hence, the relation between risk and number of facilities depends sensitively on how secure those facilities are and what capabilities terrorists have.) Reducing the number of facilities and transports also makes it possible to concentrate resources on ensuring high security at the remainder. These are the reasons why consolidation of nuclear weapons and materials at fewer sites, coupled with steps to minimize the number of transports, have been significant parts of the nuclear security agenda. (For transports, both the number of transports containing a significant fraction of a bombs' worth of material and the total time spent during such transports may be useful measures to try to minimize, as a road shipment of that takes half an hour clearly should not count as posing exactly the same risk as a road shipment that takes a week.)[49]

---

[48] The probability of any particular facility having security two standard deviations below the mean in a normal distribution is 2.275%. Hence the probability of not having one such facility in five would be $1-(1-0.02275)^5=0.109$; the probability of not having one such facility in ten would be $1-(1-0.02275)^{10}=0.206$; and the probability of not having one such facility in twenty would be $1-(1-0.02275)^{20}=0.369$.

[49] Past studies have proposed minimizing the "underway inventory," measured by the average amount shipped per year multiplied by the average duration of each shipment. See discussion in U.S. National Academy of Sciences, Panel on Reactor-Related Options, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options* (Washington, D.C.: National Academy Press, 1995; available at http://books.nap.edu/html/plutonium/0309051452.pdf as of 30 December 2006), pp. 100-101. But a shipment carrying 1,000 bombs'

To reduce the uncertainty in estimating the parameter $P_{os(j,k)}$, it would be important to collect information, to the extent possible, on:

- The location and characteristics of all facilities worldwide where at least one nuclear weapon or significant fraction of the amount of nuclear material needed for a bomb are located, as well as transportation practices worldwide for these items;
- Security levels for each such facility and transportation leg worldwide, including the kinds of threats security measures are designed to protect against; the technical measures in place for such protection; the number, quality, and capability of personnel, including guards, for such protection; and the dedication, morale, and "security culture" of the personnel important to security;
- Indicators suggesting the level of capability terrorists or criminal groups might be able to bring to bear in each of the countries where these facilities or transportation legs exist, including the magnitude of outsider attacks and crimes (both nuclear and non-nuclear that have already taken place in that country (or in similar countries in its region.

The Probabilities of Insider Theft Attempts, $P_{i(j)}$ and $P_{is(j,k)}$

As with outsider theft attempts, the probability that a group will decide to undertake an insider theft attempt, $P_{i(j)}$ is presumably determined largely by its estimate of the probability of success on that route – that is, its estimate of $P_{is(j,k)}$. $P_{is(j,k)}$ is the combination of the probabilities of success of two separate steps: the probability that the terrorist group would be able to get one or more insiders to participate in a nuclear theft attempt (either by infiltrating members or affiliates into the staff of a targeted organization, or by convincing existing insiders to take part, for example by ideological persuasion, bribery, or blackmail), $P_{ir(j,k)}$, and the probability that those insiders will then succeed in carrying out the nuclear theft, $P_{it(j,k)}$:

$$P_{is(j,k)} = P_{ir(j,k)} \times P_{it(j,k)}$$

To maximize $P_{it(j,k)}$, a group would presumably attempt to identify facilities with the weapons or materials it wanted, assess their security levels as best it could, and choose one which it judged had the best combination of good quality material and modest security to maximize the group's overall chances of success in getting a nuclear bomb. Most of the discussion above with respect to outsider threats – including the importance of the capability of the security measures at the site compared to the capability the adversaries can bring to bear – is also relevant for insider threats and essentially the same techniques of vulnerability assessment are used to assess the adequacy of facilities' protection against each type of threat. For an insider theft attempt, terrorists would also have to factor in an estimate of $P_{ir(j,k)}$, their chances of getting one or more insiders to participate in a theft attempt. Until they have an insider at a particular facility, terrorists' information about insider-focused security measures

---

worth of material poses little more risk than a shipment carrying 3 bombs' worth of material. As each shipment carrying a bombs' worth or a substantial fraction of a bombs' worth of material represents another opportunity for theft, the total number of such shipments would be a better measure; that measure could be modified somewhat with a measure of total time on the road for such shipments (since a weeklong trip clearly creates more opportunities than a 1-day trip, though probably not seven times as many).

is likely to be even more imperfect than their information about security against outsider thefts, for the key measures dealing with insiders (from vaults and security cameras to rules ensuring that no one is ever alone with nuclear weapons or material) are more difficult to observe from outside the facility. Insiders themselves, however, will in many cases be able to observe the security arrangements at their facility in much greater detail than terrorist outsiders can and will presumably be far more likely to choose to make a theft attempt (whether instigated from without or on their own initiative) at a facility where they judge the security is poor enough to give them a good chance of success.

As with $P_{o(j)}$, $P_{i(j)}$ is presumably small; while there are quite a number of confirmed insider thefts of nuclear material in the historical record, there are few that appear to have been instigated by terrorists. As noted in Chapter 2, a Russian criminal trial in 2003 revealed that a Russian businessman had been offering $750,000 for stolen plutonium for sale to a foreign client and had attempted to instigate an insider plutonium theft by making contact with residents of the closed nuclear city of Sarov, who claimed to have the access necessary to steal plutonium;[50] this was clearly an effort to instigate insider theft and may have been terrorist-linked. The Japanese terror cult Aum Shinrikyo reportedly attempted to get a meeting with the Russian Minister of Atomic Energy to offer to buy a nuclear weapon;[51] while bizarre and doomed to failure, this should probably also be considered in the category of a terrorist acquisition attempt focused on persuading an insider to provide a nuclear weapon.

To maximize its overall chances of success, the terrorist group would also want to maximize $P_{ir(j,k)}$, the chance of being able to get one or more insiders to participate in a nuclear theft. Hence, in addition to security levels and threat levels, discussed previously, the probability of a successful insider theft is presumably also related to (a) the quality of personnel reliability programs, designed to ensure that employees are trustworthy before they are hired and monitor them afterward to ensure that they remain so; (b) rates of corruption and theft among insiders at the relevant facilities; (c) low morale among those insiders; (d) low pay for those insiders; and (e) support for extreme causes among insiders, particularly causes similar to those of groups that are members of N_n. These are among the reasons why incidents of low pay and morale in the nuclear and military establishments in Russia, along with corruption and theft (including theft and sale of major armaments) have provoked such international concern.[52] But the 2004 case in Northern Ireland in which a gang reportedly

---

[50] "Russian Court Sentences Men for Weapons-Grade Plutonium Scam," trans. BBC Monitoring Service, *RIA Novosti*, 14 October 2003; "Russia: Criminals Indicted for Selling Mercury as Weapons-Grade Plutonium," trans. U.S. Department of Commerce, *Izvestiya*, 11 October 2003; "Plutonium Con Artists Sentenced in Russian Closed City of Sarov," *NIS Export Control Observer* (November 2003; available at http://cns.miis.edu/pubs/nisexcon/pdfs/ob_0311e.pdf as of 23 December 2006).

[51] Matthew Bunn and Anthony Wier, with Joshua Friedman, "The Demand for Black Market Fissile Material," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/cnwm/threat/demand.asp as of 2 January 2007).

[52] For an extended list of such incidents, see Matthew Bunn, "Anecdotes of Insecurity," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing

linked to the Irish Republican Army stole tens of millions of dollars from a bank vault that required two officers of the bank to open – by kidnapping the families of two officers of the bank and blackmailing those officers to participate – is an important reminder that insider thefts can occur even if the system is designed to prevent thefts by any lone employee and the employees themselves are not untrustworthy.[53]

Insiders could play a wide range of roles in an attempted nuclear theft. An insider or group of insiders could carry out the theft themselves, either covertly (which they would presumably prefer) or overtly (an approach that would likely require violence of the threat of violence). Alternatively, insiders could help outsiders (ranging from simply providing information about the security system and its weaknesses at one extreme to active and violent participation on the other, such as killing one or more of the guards to help the outsiders overcome them). Insiders could include people with access to nuclear material, guards, managers, or others.

The effect of improved insider security measures on reducing $P_{is(j,k)}$ – both measures to reduce the chance of insider participation and measures to reduce their chances of success if they do – could be assessed using this model in much the same way as described above in the case of the outsider threat. As in the outsider case, assumptions about the initial level of terrorist capability and their ability to increase that capability are crucial to assessing how much difference a particular set of improved security measures would make. If it is assumed that personnel reliability programs and other measures make it extremely unlikely that there would be more than one insider, then limited security measures intended to defend against one insider would be effective in defending against nearly all of the likely threat; if, on the other hand, insider conspiracies of 3-5 individuals are a real possibility, then the required security measures will be far more expensive and less certain of success.

Effect of the Quantity of Material and Facility Throughput

The danger of insider theft may be somewhat more closely related to the quantity of material at a site than the danger of outsider theft. For insider theft, there is likely to be a high premium on remaining covert (at least until the theft is completed) and the chance of remaining covert is at least related to the quantity of material: a theft of 50 kilograms of HEU would be more likely to be noticed at a site where that was all the HEU on hand than at a site where there were many tons of HEU.

But even more important than the sheer quantity of material is the degree to which the material is being handled and processed: if material is simply sitting in a secure vault monitored with security cameras at all times, insider theft is likely to be quite difficult, whereas if the facility is doing extensive hands-on processing of tons of material each year,

---

the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/threat/anecdote.asp as of 2 January 2007).

[53] For a discussion of the Northern Bank case, see, for example, Chris Moore, "Anatomy of a £26.5 Million Heist," *Sunday Life*, 21 May 2006. Chris Ward, one of the bank officers whose families were held hostage, has since been arrested and charged with willing participation in the crime, which he denies. If he was a willing participant, it appears that he was motivated by republican sympathies, again highlighting the importance of sympathies for causes similar to those of terrorist groups among employees of a protected facility.

removal of a few kilograms, in small bits at a time, would have a much greater chance of going unnoticed. (Annual throughput might provide a rough metric for assessing this aspect of a facility.)

Effect of the Number of Personnel

The probability of successful insider theft is likely to be closely related to the number of insiders in a position to steal nuclear material (or to be of substantial assistance in doing so). If nuclear material is stored in a vault to which almost no one has access, the probability of insider theft is far lower than if hundreds of people have regular access to it. The more people have access to the material, or have enough knowledge of the security system to be able to help outsiders defeat it, the more chances there are for there to be a bad apple among them.

To reduce the uncertainty in estimating the parameter $P_{is(j,k)}$, it would be important to collect information, to the extent possible, on:

- The location and characteristics, as before, of all facilities worldwide where at least one nuclear weapon or significant fraction of the amount of nuclear material needed for a bomb are located, as well as transportation practices worldwide for these items;
- Security levels focused on protection against insider theft for each such facility and transportation leg worldwide, including the kinds of insider (and combined insider-outsider) threats security measures are designed to protect against; the technical measures in place for such protection; the number, quality, and capability of personnel, including guards, for such protection; the procedures taken to ensure the reliability of personnel; and the dedication, morale, and "security culture" of the personnel important to security;
- The number of people in each such facility or transportation leg with the access required to steal a nuclear weapon or nuclear material, or to contribute substantially to doing so, and the circumstances of such access (e.g., is the material being processed in bulk by hand on a daily basis, or sitting in a rarely used and closely monitored vault);
- Indicators of theft risks among insiders, including low pay and morale; corruption; insider thefts of non-nuclear items at the same or similar facilities or institutions; and adherence to extreme ideologies compatible with those of potential nuclear terrorist groups;
- Indicators suggesting the level of capability insiders (and insiders working with outsiders) might be able to bring to bear in each of the countries where these facilities or transportation legs exist, including the capability shown in insider thefts (both nuclear and non-nuclear) that have already taken place in that country (or in similar countries in its region).

The Probabilities of Black-Market Acquisition Attempts, $P_{b(j)}$ and $P_{bs(j,k)}$

Trying to buy nuclear weapons or materials on a nuclear black market appears to be an especially common choice for terrorist groups seeking a nuclear capability. Both Aum

Shinrikyo and al Qaeda have pursued this route.[54] Thus $P_{b(j)}$ appears to be fairly large. In part, this may reflect opportunities for black-market acquisition presenting themselves – in the form of individuals who claim to be able to provide nuclear items, requiring a decision – in a way that opportunities for instigating an outsider or insider theft do not. In part, however, it may also reflect a judgment on the part of terrorist groups that the probability of success in getting nuclear material on the black market is substantial, perhaps better than the probability of success in instigating an outsider or insider theft.

Like insider theft, the probability of success in acquiring nuclear weapons or materials on a nuclear black market, $P_{bs(j,k)}$, can be broken into two probabilities: the probability of a potential seller coming into possession of such goods and the probability that the seller and the buyer will succeed in finding each other and making the transaction.

The principal source of black-market nuclear material is likely to be nuclear theft, by outsiders or insiders not directly instigated by terrorist groups.[55] Numerous cases of theft of weapons-usable nuclear material, apparently with the intention of selling the stolen nuclear material on the nuclear black market, have occurred. The IAEA has documented 16 seizures of stolen HEU or separated plutonium confirmed by the states concerned – and more cases exist that definitely occurred, but that the relevant states have not been willing to confirm.[56] While most of the known cases occurred in the mid-1990s, one significant seizure of stolen HEU occurred as recently as 2003, suggesting that the problem of nuclear thieves stealing material for later sale is a continuing one.

Improved nuclear security measures would reduce the probability of additional thefts of HEU and plutonium after the security measures are implemented. The critical difference between the nuclear black market option and the options of instigating insider or outsider thefts, however, is the possibility of sale of nuclear weapons or materials that may already have been stolen in the past; no security upgrades implemented now will solve that problem. The documented cases on the IAEA's list involve material that was seized and recovered, and therefore this material will not show up on a nuclear black market – but the key question,

---

[54] Bunn and Wier, "The Demand for Black Market Fissile Material."

[55] State decisions to provide nuclear weapons or the materials for them to terrorist groups are discussed separately below; state decisions to provide such items to black market middlemen, with no control over who they might then sell them to, seem so unlikely that they are not further considered here.

[56] International Atomic Energy Agency, *Illicit Trafficking and Other Unauthorized Activities Involving Nuclear and Radioactive Materials* (Vienna: IAEA, 2006; available at http://www.iaea.org/NewsCenter/Features/RadSources/PDF/fact_figures2005.pdf as of 29 January 2007). Well-confirmed cases (where the individuals involved were caught, tried, and convicted) that are not in the IAEA database include, for example, the 1992 theft of 1.5 kilograms of 90% enriched HEU from the Luch Production Association in Podolsk, Russia, and the 1993 thefts of 1.8 kilograms of 36% enriched HEU from the naval facility at Andreeva Guba and of 4.5 kilogram of material enriched to roughly 20% from the naval facility at Sevmorput, both in Russia. See, for example, "Confirmed Proliferation-Significant Incidents of Fissile Material Trafficking in the Newly Independent States (NIS), 1991-2001" (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 30 November 2001; available at http://cns.miis.edu/pubs/reports/traff.htm as of 3 March 2006).[57] U.S. National Intelligence Council, *Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces* (Washington, D.C.: Central Intelligence Agency, 2004; available at http://www.dni.gov/nic/special_russiannuke04.html as of 5 March 2005).

unfortunately unanswerable, is how many other thefts may have occurred that were not detected. The CIA assesses that additional undetected thefts probably have occurred, but no one can know how many or how substantial they may have been.[57]

Three factors suggest that already-stolen nuclear material may not be a large part of the black-market problem. First, there is no convincing evidence that al Qaeda succeeded in acquiring stolen nuclear material despite attempting to do so for many years before the 9/11 attacks, suggesting that there may not have been many stocks of already-stolen material available. Second, none of the documented seizures of stolen nuclear material to date have been confirmed to have involved nuclear material stolen long before (though when and where the material was stolen is not known for certain in all cases). Third, nuclear workers in the former Soviet Union who may have stolen nuclear material a decade ago and squirreled it away for a rainy day are now making a living wage, paid on time, suggesting that if they did not sell this material before, they may not do so now. (On the other hand, if improved security measures make it more difficult to steal nuclear material, already-stolen material could become more valuable, creating more incentives to sell it.) While these factors suggest that the fraction of the black-market problem arising from already stolen nuclear material is small, it is probably not insignificant.

The model presented here can be used to assess the impact of different assumptions about already-stolen nuclear material on the risk-reduction benefit that might be derived from upgrading security for not-yet stolen material. Consider two quite different cases. If we assume, in the first case, that only 20% of the probability of successful black-market acquisition comes from already-stolen material; that a program of security upgrades could reduce the probability of success in instigating either an outsider or an insider theft by 80% (with the same effect on thefts not instigated by a particular buyer); and that the probability of terrorists choosing each type of acquisition attempt would be unaffected by these security upgrades (perhaps because the upgrades were not observed by the terrorists), then the overall probability that an acquisition attempt would be successful, using the numbers from the numerical example above, would be:

$$P_{s(k)} = \left(0.2\times 0.2\times 0.2 + 0.3\times 0.3\times 0.2 + 0.3\times 0.2\times\left(0.8\times 0.2 + 0.2\right) + 0.2\times 0.5\right)$$
$$\left(0.4\times 0.7\right) = 0.016$$

The 10-year risk of a nuclear terrorist attack would be reduced by more than three times by such security upgrades.[58] (The risk reduction is less than the reduction in the probability of successful theft because of the contributions to risk from already-stolen material and from state provision of nuclear capabilities.)

As a second, contrasting possibility, if already-stolen nuclear material represented 60% of the initial probability of success for the black-market option, unaffected by such security upgrades, and one assumed that the terrorists would observe the security upgrades

[58] This is not intended as an argument for a particular program of upgrades that could ostensibly achieve this 80% reduction in the probability of successful theft, but only an example to illustrate how much changes in assumptions about the fraction of the risk posed by already-stolen material affect the outcome.

and put less emphasis on instigating thefts and more on black-market acquisition, then, using the same numbers, the overall probability that an acquisition attempt would be successful would be:

$$P_{s(k)} = \left(0.1 \times 0.2 \times 0.2 + 0.15 \times 0.3 \times 0.2 + 0.55 \times 0.2 \times \left(0.4 \times 0.2 + 0.6\right) + 0.2 \times 0.5\right)$$
$$\left(0.4 \times 0.7\right) = 0.027$$

In this case, the overall 10-year risk would not quite be cut in half as a result of the security upgrades – still a substantial benefit. Only if the probability that terrorists would choose to attempt to instigate either an outsider or an insider attack were close to zero *and* nearly all of the problem of black-market acquisition was the result of already-stolen material – neither of which seem especially plausible – would security upgrades that drastically reduced the probability of nuclear theft *not* result in substantial reductions in the danger of nuclear terrorism. Hence, the model strongly suggests that while some horses may already be out of the barn, closing the door on the remainder would have very real risk reduction benefits.

In the black-market case, potential sellers getting hold of a nuclear weapon or the materials to make one is only the first step. In the next step, they would have to make contact with, and succeed in closing a transaction with, buyers from a terrorist group – and that is not likely to be easy. None of the known cases involving stolen HEU or plutonium appears to have involved a real buyer, or come close to a successful transaction. This may be the product of selection bias; it could be that the competent thieves and smugglers connected to buyers are the ones who did not get caught and whose cases are therefore not known. If selection bias only distorts the picture modestly, however, the known cases suggest that the problem of making the connection between potential buyers and sellers – with the risks each faces that the other may be a scam artist, killer, or government agent – is a major barrier on this path and the chances of success in such a transaction are relatively low.[59]

In particular, the record seems to suggest a large number of cases of scams, in which sellers attempted to pawn off worthless material they described as "red mercury" and other radioactive trash as weapons-usable nuclear material. A case could be made, based on this record, that the 20% chance of successful black-market acquisition in the numerical example is too high; on the other hand, hand-held equipment which can confirm the presence of HEU or separated plutonium in a container is commercially available at modest cost, suggesting that sophisticated buyers are likely to become less and less susceptible to scams over time.

How could the probability of successful black-market acquisition be further reduced? Measures to prevent outsider and insider theft are the first priority, as already discussed. Next

[59] The argument that the difficulty of making the connection between potential sellers and potential buyers in this market is one of the major factors that has prevented nuclear terrorism to date is made in "Nuclear Terrorism: Why Hasn't It Happened Already?" in Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007), p. 27. For another recent discussion of these difficulties, see, for example, Langewiesche, "How to Get a Nuclear Bomb."

in priority are measures to make the barriers to successful transactions between buyer and seller even higher than they already are. Intelligence and law enforcement agencies could run additional stings and scams, posing as either buyers or sellers of nuclear material, to catch participants in this market, collect intelligence on market participants, and increase the fears of real buyers and sellers that their interlocutors may be government agents. As most of the confirmed cases in which stolen weapons-usable nuclear material was successfully seized involved one of the conspirators or some one they tried to involve in the effort informing on the others, additional measures to make such informing more likely – including anonymous tip hotlines that were well-publicized in the nuclear community, rewards, and the like – could also have substantial benefit. All potential source states and likely transit states should have units of their national police force trained and equipped to deal with nuclear smuggling cases, and other law enforcement personnel should be trained to call in those units as needed. Current efforts to put in place radiation detection at key border crossings may also reduce risk, forcing smugglers to pursue more difficult and chancier routes.[60]

To reduce the uncertainty in estimating the parameter $P_{bs(j,k)}$, it would be important to collect information, to the extent possible, on:

- All the factors mentioned above that help determine the probabilities of outsider and insider thefts;
- Data that may help clarify the likelihood that significant quantities of nuclear material may have been stolen in the past that may still be offered for sale in the future (including interviews with individuals known to have been nuclear thieves or to have attempted to purchase stolen nuclear materials; assessments of how much material could potentially be missing from different sites given past and ongoing accounting uncertainties; assessments, in recent cases of seized nuclear material, of whether the material had been stolen recently or long before; and interviews with selected individuals at key previously vulnerable facilities to determine if they have any knowledge of past incidents of nuclear theft that may have gone unreported);
- Data that may help clarify the chances of illicit nuclear buyers and sellers successfully making contact with each other (in particular, through the kinds of sting operations mentioned above, which can document how difficult it is for a buyer or a seller who happens to be a government agent to successfully locate a real buyer or seller to interact with);
- Data that may help clarify the chances of smugglers being able to ship nuclear material across borders (as might be collected, for example, through officially sponsored "red team" tests of how easy or difficult it was to do so).

[60] For a discussion of measures in this area and their strengths and weaknesses, see Anthony Wier, "Interdicting Nuclear Smuggling," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/cnwm/interdicting/index.asp as of 1 March 2005).

The Probabilities of Acquisition From Nation-States, $P_{n(j)}$ and $P_{ns(j,k)}$

The last option for attempting to acquire a nuclear weapon or weapon-usable nuclear materials is from a state in possession of such items. President George W. Bush is among those who see this acquisition path as the dominant danger: "Rogue states," he has said, "are clearly the most likely sources of chemical and biological and nuclear weapons for terrorists."[61] This belief determines the policy prescription: if the principal danger of terrorists acquiring weapons of mass destruction is that hostile states might provide them, then the key element of the solution is to take on those hostile states and make sure that they do not provide them. This is the idea that animates the preemptive doctrine laid out in the 2002 and 2006 editions of the administration's *National Security Strategy* and that was fundamental to the argument for going to war with Iraq.

It is certainly *not* correct, as is sometimes argued, that only terrorists with help from a state could possibly put together the capability to get and use a nuclear bomb.[62] Under all but a few circumstances, states are extremely unlikely to consciously decide to transfer a nuclear weapon or weapons-usable nuclear materials in their possession to a terrorist group. Such a decision would mean transferring the most awesome military power the state had ever acquired to a group over which it had little control – a particularly unlikely step for dictators or oligarchs obsessed with controlling their states and maintaining power. If the terrorists actually used the transferred capability against the United States or one of its allies, there would be a substantial chance that the source of the weapon or material would be traced back to the state that provided it and that the resulting retaliation would be overwhelming, almost certainly removing the government that decided on such a transfer.

Hence, prior to the 2003 U.S.-led invasion of Iraq, U.S. intelligence agencies reportedly unanimously concluded that it was unlikely Baghdad would attempt any form of unconventional attack on the United States except if "ongoing military operations risked the imminent demise of his regime" or if he intended to "extract revenge" for such an assault; the only dissent was from the State Department, who thought Saddam Hussein would not attempt such an attack even then.[63] Similarly, given the importance Pyongyang appears to attach to regime survival, it appears extremely unlikely that North Korea would take the risk of providing nuclear materials or weapons to terrorists unless the regime concluded that U.S. overthrow of the regime was inevitable – or became so desperate that the revenue from a nuclear sale came to be seen as crucial to regime survival. A decision by the Iranian government to provide nuclear weapons or materials to al Qaeda terrorists (in the future, when the Iranian government might have such items to provide) also appears extraordinarily unlikely, particularly as the Sunni al Qaeda has been sponsoring widespread attacks on Shiites in Iraq, Pakistan, and elsewhere.

---

[61] President George W. Bush, "President Speaks on War Effort to Citadel Cadets: Remarks by the President at the Citadel" (Washington, D.C.: The White House, Office of the Press Secretary, 11 December 2001; available at http://www.whitehouse.gov/news/releases/2001/12/20011211-6.html as of 5 March 2006).

[62] Bunn and Wier, *Securing the Bomb: An Agenda for Action*, pp. 25-26.

[63] Murray Waas, "Intel Reports Cast Doubt on Iraq War Justifications," *Global Security Newswire*, 9 March 2006 (available at http://www.nti.org/d_newswire/issues/2006/3/9/541C9625-EB23-4F5F-8A47-1663B968B897.html as of 13 March 2006).

These are the reasons why, in the numerical example above, the probability of success for an attempt to get nuclear weapons or materials from a nation-state, $P_{ns(j,k)}$, was assumed to be quite low (5%). As there is no historical evidence of any terrorist attempt to acquire nuclear weapons or materials from states, it may be that the 20% probability of terrorists choosing to pursue this route used in the numerical example above is too high – though the absence of publicly available confirmation of such incidents does not prove that they have not occurred.

Steps to reduce the probability of success for attempts to get nuclear weapons or materials from nation-states would include: (a) efforts to put together a package of carrots and sticks that would convince the governments in Pyongyang and Tehran that it was in their national interest to give up their nuclear ambitions (along with any nuclear weapons or weapons-usable nuclear material North Korea may already have), so that they did not have nuclear weapons or weapons-usable material available to transfer even if they wished; (b) steps to convince states that the United States would have a good chance of tracing the origin of nuclear material used in a terrorist nuclear attack and would be very likely to launch a devastating retaliation against the state that provided such items; and (c) steps to ensure that states in a position to make such transfers do not become sufficiently desperate that such transfers might be seen either as the last chance for regime survival or the last chance to punish those whose actions led to the regime's collapse. Efforts such as the Proliferation Security Initiative (PSI) and improved border controls, designed to increase the chance that such a transfer could be intercepted, should also be pursued – but given that the nuclear materials for a bomb could easily fit into a briefcase and are quite difficult to detect, such efforts are likely to be able only to have a modest effect on the probability of successful transfers.

To reduce the uncertainty in estimating the parameter $P_{ns(j,k)}$, it would be important to collect information, to the extent possible, on:

- Past decision-making in key states such as Iraq, North Korea, and Iran relating to cooperation with terrorists (and in particular cooperation related to weapons of mass destruction);[64]
- Past decision-making by terrorist groups such as al Qaeda and Aum Shinrikyo concerning whether to attempt to convince a state to provide weapons of mass destruction (potentially available from interviewing arrested former operatives of these groups); and
- Data on the difficulty of organizing a sale and physical transfer of a nuclear weapon or nuclear materials from a developing state to a terrorist group (as might be acquired in part through simulations and exercises).

[64] Considerable information on the Iraqi case may now be available from interviews with former senior officials and from documents recovered after the 2003 war. The CIA's investigator, however, does not mention any significant policy discussions on the subject. See Charles Duelfer, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at https://www.cia.gov/cia/reports/iraq_wmd_2004/index.html as of 10 December 2006). Information on decision-making in North Korea and Iran would be very difficult to collect at present, but might become more available were these governments to change in the future.

The Probability Terrorists Could Make a Nuclear Bomb or Detonate a Stolen Nuclear Weapon, $P_{w(j,k)}$

As discussed in Chapter 2, getting the nuclear material is the most difficult part of making a nuclear bomb – but making a workable bomb from most types of stolen material is not a trivial matter. Most of the world's terrorists would have little chance of being able to make a nuclear bomb, even if they had the nuclear material to do so. But the question of whether a terrorist group could make a nuclear bomb only becomes relevant if the group is sufficiently well-organized, well-financed, and sophisticated to have succeeded in acquiring a sufficient quantity of weapons-usable nuclear material. What is important, then, is not the probability of success for all terrorist groups, including tiny cells with little capability to do more than a truck bomb at a bar, but the probability of success for the small subset of terrorist groups within the set N_n, which includes only groups at the high-capability tail of the distribution of terrorist capabilities.

As described in Chapter 2, unfortunately, with enough weapons-usable nuclear material in hand, it does not take the resources of a state to design and build a crude unsafe, unreliable nuclear bomb of uncertain yield, capable of being delivered in a van or yacht – which may be all a terrorist group requires. A sophisticated group that had devoted the level of organizational focus and resources required to get enough weapons-usable nuclear material for a bomb would presumably also have devoted significant organizational resources to pulling together the capabilities needed to make use of that material. Hence, for the small subset of high-capability terrorist groups in the set N_n, the probability of success in taking nuclear material they had acquired and making it into a bomb that would detonate when desired is probably substantial. That probability is probably less than even, but may be in the range of the 40% used in the numerical example above. Fortunately, there is no record of multiple cases of terrorists getting the material to make a nuclear bomb and attempting to make bombs from it to draw on in estimating the value of this parameter.

In most cases, a terrorist group would first transport nuclear material from wherever it was acquired to a safe location where it planned to do the work of manufacturing it into a bomb and then do the actual manufacturing.[65] The safe location might be in one of the dozens of "stateless zones" around the world where governments have minimal control (such as substantial areas of Afghanistan and Pakistan),[66] or it might be in an apparently ordinary machine-shop or chemical shop in any country in the world (including, potentially, the target

---

[65] As noted in Chapter 2, such transportation may not be essential in all cases. DOE security regulations require facilities with nuclear material that would be especially attractive to terrorists to be able to prevent terrorists from even being able to get into the building, to avoid the possibility that they could make a crude bomb while still in the building.

[66] The CIA estimates that there are some 50 "stateless zones" in the world and that "in half of these, terrorist groups are thriving." See George J. Tenet, Director of Central Intelligence, testimony in Committee on Armed Services, *Current and Future Worldwide Threats to the National Security of the United States*, U.S. Senate, 108th Congress, 2nd Session, 9 March 2004.

country).[67] Thus the probability of making a working bomb, $P_{w(j,k)}$, can be broken into two separate probabilities – the probability of success in transporting the material to the planned safe location and the probability of success in manufacturing a bomb.

Today, the probability of success in transporting the material to a planned safe location is probably quite high. Effective nuclear material detectors are installed and in use at only a limited number of border crossings around the world and are quite observable where they are installed, allowing terrorists and smugglers to choose other routes. Efforts to install nuclear detectors at key border crossings, to make it more difficult for terrorists to transport such items from wherever they acquire them to a safe location where they can work on them, should continue – but the nuclear materials for a bomb would fit in a suitcase, their radiation is weak and difficult to detect, and nuclear terrorists and smugglers are likely to pick unmonitored routes. It would also be desirable to put in place more effective and practiced procedures for responding to the discovery of a nuclear theft that had just occurred – rapid approaches to searching the area immediately around the facility and questioning facility personnel; rapid deployment of nuclear detectors on roads and rail-lines leading away from the area and at nearby airports; immediate steps to inspect all shipments leaving the country for nuclear material; and more. But it would be unwise to put undue reliance on such measures.

As discussed in detail in Chapter 4, the probability of success in manufacturing a crude bomb will depend on the quantity and quality of nuclear material the terrorist group acquires. If the group managed to get a sufficient quantity of HEU metal (or HEU in forms it had the capability to convert to metal), it could make a simple "gun-type" bomb, in which two pieces of HEU (each less than a critical mass by themselves) are slammed together at high speed. If, on the other hand, the group had acquired plutonium, or an amount of HEU too small for a gun-type device, the group would have to attempt the more challenging task of building an "implosion-type" bomb, in which explosives arranged around a ball of nuclear material are detonated so as to crush the ball to a higher density, setting off the nuclear chain reaction.

Building an implosion bomb would be a significantly greater challenge for a terrorist group, and the probability of success in doing so would be significantly lower than the probability of successfully building a gun-type bomb. For this reason, some analysts have argued for a policy that would focus primarily on securing HEU stockpiles, giving plutonium, which cannot be used to make an effective gun-type bomb, a lower priority.[68] But a strong case can be made that, while making an implosion bomb is substantially more difficult, many of the groups with the sophistication needed to acquire weapons-usable nuclear material and make it into a gun-type bomb would also be able to succeed in the task of acquiring the

---

[67] For a scenario in which this activity takes place on an isolated farm in the United States (to avoid having the noise from non-nuclear testing of the gun raise alarms), see Peter D. Zimmerman and Jeffrey G. Lewis, "The Bomb in the Backyard," *Foreign Policy*, no. 157 (November/December 2006), pp. 32-39.

[68] Charles D. Ferguson and William C. Potter, with Amy Sands, Leonard S. Spector, and Fred L. Wehling, *The Four Faces of Nuclear Terrorism*, ed. Amy Sands, Leonard S. Spector, and Fred L. Wehling (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004; available at http://www.nti.org/c_press/analysis_4faces.pdf as of 2 January 2007).

additional capabilities needed to make an implosion-type bomb; that is to say, the probability of success might be only 40-60% as high as for an implosion-type bomb, but it is not likely to be only 0-5% as high.

Similarly, while the need to do some chemical processing if the group acquires nuclear material in forms other than the metal form preferred for use in a bomb would be an additional barrier (and create additional risks that the group's work might be detected before it was finished), the reduction in the chance of success for many important forms of nuclear material that a group might acquire would be significant but is not likely to be anything like an order of magnitude.

Terrorists would require some 50-60 kilograms of weapons-grade HEU for a gun-type bomb (or more, if the material was less enriched). Substantially less material would be needed for a crude implosion-type bomb: the Nagasaki implosion bomb, for example, involved approximately 6 kilograms of plutonium. A comparable weapon using weapon-grade HEU would require roughly three times more.[69]

Policy approaches to reducing the probability of successful manufacture of a bomb would include (a) strengthened intelligence, law-enforcement, and counter-terrorist measures that could increase the chance of stopping an effort to pull together the needed capabilities while it was still in progress, make it more difficult for groups to recruit the needed technically skilled personnel, and increase the chance of detecting such efforts, as discussed above; (b) intelligence collection focused on particular indicators of this type of activity, ranging from purchase of some of the books that would be most useful to a crude nuclear weapons designer, to acquisition of certain types of high-temperature crucibles for casting metal parts from uranium or plutonium, to release of certain types of slightly radioactive effluents (including greatly expanded cooperation with other countries to help them put in place capabilities to detect such activities); and (c) efforts to rebuild failed states, avoid future failed states, and help countries gain control over "stateless zones." Such measures, however, are not likely to cut the terrorists' chances of success dramatically: while strengthened intelligence efforts are needed, as discussed in Chapter 2, the activities in putting together a nuclear bomb may be small and easy to hide. And while limiting terrorists' access to sanctuaries where they could work on a bomb program will have some impact on reducing the risk of nuclear terrorism, such a program would also have a significant chance of being carried out undetected in a machine-shop in any country in the world.

---

[69] The critical mass of 93% enriched HEU is approximately three times that of weapon-grade plutonium in its most commonly used delta phase. See, for example, H.C. Paxton and N.L. Pruvost, *Critical Dimensions of Systems Containing 235U, 239Pu, and 233U: 1986 Revision* (Los Alamos, N.M.: Los Alamos National Laboratory, 1987; available at http://www.fas.org/sgp/othergov/doe/lanl/lib-www/la-pubs/00209019.pdf as of 9 January 2007), pp. 97, 102.

To reduce the uncertainty in estimating the parameter $P_{ns(j,k)}$, it would be important to collect information, to the extent possible, on:

- The chances of success in transporting nuclear material to potential safe locations (as might be gathered through simulations and exercises involving attempts to make such transports);
- The current level of nuclear knowledge among groups plausibly in the set N_n (an assessment that has been a high intelligence priority for a long time, but which is very difficult to make);
- The numbers and skills of personnel, types of equipment, and types of processes likely to be needed for various different approaches to manufacturing a crude bomb (including an assessment of those actually used for initial bomb manufacture, and any problems encountered, in selected cases of state nuclear programs);
- The chances of success in recruiting personnel with the skills needed to manufacture a crude bomb (which could again be assessed through exercises in which attempts to do so were made);
- The chances of success in acquiring the needed equipment without detection (which could similarly be assessed through exercises, among other approaches);
- The types of mistakes that might be made, and difficulties that might arise, in terrorists' efforts to process nuclear material and manufacture a nuclear bomb (which could conceivably be assessed through simulations and exercises);
- The chances of success in avoiding detection during the actual manufacturing process if it were conducted on the territory of a failed state or in a stateless zone; and
- The chances of success in avoiding detection during the actual manufacturing process if it were conducted in a covert facility in a functioning state.

A terrorist group that got hold of a stolen nuclear weapon would face somewhat different challenges. As discussed in Chapter 2, weapons equipped with modern, difficult-to-bypass electronic locks, environmental sensing devices, and the like might be quite difficult for a terrorist group to figure out how to detonate. Older weapons not equipped with such features would pose a smaller challenge, but still a significant one. Terrorists trying to detonate such a weapon could benefit substantially from help from a knowledgeable insider – but even that might not be enough, as the electronic locks are specifically intended to prevent insiders from being able to set the weapons off without authorization. If they could not figure out how to detonate a stolen weapon, terrorists might choose to remove the nuclear material from it and seek to fashion it into a bomb. In any case, terrorists who had a stolen nuclear weapon would be in a position to make fearsome threats—for no one would know for sure whether they could set it off or not.

The Probability Terrorists Would Deliver a Nuclear Bomb, $P_{d(j,k)}$

Unfortunately, the chance that terrorists could successfully smuggle a nuclear bomb into any major country is high, despite the nuclear detection measures that have been put in place since 9/11. Attempting to protect the United States from nuclear terrorism by detecting and stopping nuclear contraband at the U.S. borders is like a football team defending at its own goal line – but with that goal line stretched to thousands of kilometers, much of it unguarded wilderness, with millions of people and vehicles legitimately crossing it every year.[70] Moreover, while Osama bin Laden has spoken of using nuclear, chemical, or biological weapons for "deterrence," the chance that a group that went to the effort involved in getting a nuclear bomb would decide to use it seems likely to be high. These are the reasons for the 70% estimate, used in the numerical example above, for the probability that terrorists would decide to, and be able to, deliver and detonate a nuclear bomb should they succeed in making one.

Policy options for reducing this probability would include (a) beefing up detection and interdiction capabilities at all national borders (as well as within potential target countries); (b) steps to attempt to deter terrorists from using such a capability; and (c) efforts to make the case within the communities from which terrorists draw support that the use of nuclear weapons to murder innocents on a mass scale is morally illegitimate. Each of these approaches might reduce the risk by a few percent; only the last, however, seems to have any significant hope of having a larger impact.

To reduce the uncertainty in estimating the parameter $P_{d(j,k)}$, it would be important to collect information, to the extent possible, on:

- The chances of success in transporting a nuclear weapon into potential target countries by various routes (as might be gathered through simulations and exercises involving attempts to make such transports); and
- The thinking of terrorist groups that might be within the set N_n concerning the actual use of weapons of mass destruction, should they acquire them.

The Consequences of a Terrorist Nuclear Attack, C_c

The consequences of a terrorist nuclear blast – turning the heart of any major city into a modern Hiroshima – are almost too horrible to contemplate. Tens or hundreds of thousands of people could be killed, with total economic costs in the trillions of dollars. As noted above, the worldwide economic repercussions could drive a global economic depression, affecting countries far beyond the borders of the state attacked. Terrorists might exert blackmail or cause panic by claiming to have a second bomb. The reaction after such an attack is difficult to predict but would almost certainly by ugly. The world as we know it would be changed profoundly. It is difficult to monetize all of these consequences, but it is clear their magnitude is large; the $4 trillion estimate used in the numerical example above may even be an understatement.

---

[70] For useful discussions, see Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*; Wier, "Interdicting Nuclear Smuggling."

A substantial fraction of the damage from a nuclear blast is immediate and no amount of preparedness ahead of time would reduce it. There are, however, steps that could be taken to reduce some of the consequences, if nations chose to make substantial investments in doing so – ranging from resilient arrangements to ensure continuity of government and of critical private business operations, to preparing to provide massive surge capacity for treating burn and radiation victims, to better plans to evacuate people from the projected path of the radioactive fallout.

To reduce the uncertainty in estimating the parameter C_c, it would be important to collect information, to the extent possible, on:

- The likely casualties and direct economic damage resulting from nuclear blasts in different potential target cities;
- The likely effects of such a blast on government and economic actors' ability to function effectively;
- Capabilities in place to evacuate populations in a timely way, treat the burned, irradiated, and wounded, and to recover and reconstruct (including what responses to other large-scale recent disasters, such as Hurricane Katrina, may have to say about such capabilities);
- Steps terrorists might take to blackmail the target country or sow panic in the wake of such an attack; and
- Likely follow-on economic impacts of such an attack.

The Dynamics of the System

As described in Chapter 5, national systems for securing nuclear stockpiles and the global system that is the aggregation of those national systems are strongly incident-driven. When the attack on the Munich Olympics in 1972 demonstrated that a carefully planned attack by a well-trained, well-armed terrorist team in the middle of a developed state like Germany was a realistic threat, the United States and a number of other countries significantly upgraded nuclear security. When stolen HEU and plutonium began turning up in Europe in the mid-1990s, major international cooperative programs were launched to attempt to beef up security and accounting for nuclear weapons and materials in the former Soviet Union. After the 9/11 attacks, the United States beefed up nuclear security at its own facilities and sought to accelerate cooperation with Russia to do the same, and a number of other countries also toughened their nuclear security rules. Nevertheless, as described in Chapter 2, scores of facilities around the world remain dangerously insecure.

Were there to be a well-documented frontal assault on a nuclear facility by a terrorist team, this would almost certainly lead to major increases in investments against protection from such outsider attacks at facilities around the world. Similarly, an acknowledged and well-documented insider theft perpetrated by a conspiracy of several insiders working together would likely cause countries around the world to review their requirements for protecting against such insider thefts. (The nuclear thefts that have taken place to date have typically been perpetrated by individual outsider or insider thieves, with no connection to

particular terrorist groups; most nuclear facilities around the world believe they are already sufficiently protected against modest threats of that kind, so these thefts did not have a comparable galvanizing effect.)

At the same time, as discussed above, terrorists will take note of increased security measures being put in place and can either shift to target facilities where comparable upgrades have not taken place; attempt to recruit more people, acquire stronger weaponry, and develop better plans and training, so as to take on the enhanced security measures; or turn to any of the wide range of terrorist options other than attempting to get and use nuclear explosives (the latter being the best success that a nuclear security system can hope for). Over time, if major incidents do not occur again, complacency is likely to set in, nuclear security measures are likely to relax, and vulnerabilities will begin to increase again. Thus, the choices of states to invest in nuclear security and terrorists to choose their strategies in response represent a long-term strategic game with many moves – a game that is likely to last as long as nuclear weapons and their essential ingredients coexist in the world with terrorist groups bent on wreaking mass destruction.

Conclusions

The model presented here cannot, in itself, eliminate the huge uncertainties in estimating the risk of nuclear terrorism. But as this chapter has attempted to show, the use of such a model can break the problem into one of estimating a series of parameters for which (in many cases) at least some basis for judgment exists – in technical analysis or historical experience or both – and can help identify additional pieces of information that could reduce the uncertainty in estimating each of those parameters. It also makes it possible to identify policy options to modify each of the parameters to reduce the risk and to explore quantitatively what the effect of such policy options might be.

Overall, the result is not surprising: it appears that the most promising policy options are based on a forward defense, combining strengthened counter-terrorism policies that could both reduce the number of groups contemplating nuclear violence and their likely effectiveness with a rapid global campaign to beef up security or remove the nuclear stocks from the world's most vulnerable sites. Once terrorists have gotten hold of a nuclear weapon or the materials to make one, the policy options available to reduce the danger that they will commit nuclear terrorism become far more limited. The great advantage of policies focused on keeping nuclear weapons and materials locked down at their sources is that the nations in control of these items know where they are; getting the job of putting in place improved security in place done is a matter of diplomacy, political will, and allocation of resources, not a matter of searching for a needle in a haystack. But once a nuclear weapon or the nuclear material to make one has walked out the door, it could be anywhere and the problems of finding and recovering it multiply a thousand-fold.

The uncertainties in estimating the risk are large, but even a risk dramatically smaller than that estimated in the numerical example used here would justify a broad range of actions to reduce the threat. And the very uncertainty of the danger highlights what we do not know –

including the possibility that a major nuclear theft could be in the planning stages at any time. There is, in short, no time to lose.

4. Identifying the Highest Risks of Nuclear Theft

On 22 August 2002, the United States government, working with the governments of Yugoslavia and Russia, the International Atomic Energy Agency (IAEA), and the private Nuclear Threat Initiative (NTI), helped to airlift 48 kilograms of highly enriched uranium (HEU) from the Vinca Institute of Nuclear Sciences in Belgrade to a secure facility in Russia, where it was blended down to low-enriched uranium.[1] The operation was carried out under intense security, with 1,200 armed Yugoslav and Serb troops guarding the material as it made its way to the airport. Characterizing the material as sufficient for two and a half nuclear bombs, the State Department hailed the operation as a major victory in the struggle to keep nuclear weapons material out of terrorist hands.[2]

But had the identical material been physically located at a U.S. research reactor regulated by the Nuclear Regulatory Commission (NRC), it would have required few security measures – because nuclear materials at research reactors are exempt from all but the most basic NRC physical protection requirements.[3] Similarly, if the Vinca material had been located at a U.S. Department of Energy (DOE) facility, it would have been considered only Category II material, requiring relatively modest security measures (though more than those required at an NRC-regulated research reactor) – because of internal DOE rules on how the dangers of theft posed by different types of material should be ranked, which are starkly different from the categorization systems the United States insisted on in international standards such as the International Atomic Energy Agency (IAEA) recommendations on physical protection and the physical protection convention.[4] While these DOE rules are in the process of being reconsidered, they remained in force as of the end of 2006.

---

[1] For an account of the Vinca operation, see Philipp C. Bleek, "Project Vinca: Lessons for Securing Civil Nuclear Material Stockpiles," *Nonproliferation Review* (Fall-Winter 2003; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/NonProRev-Bleek.pdf as of 28 September 2005). For a discussion that puts this operation in the context of several others, and makes recommendations for streamlining the process of such removals of nuclear material in the future, see Philipp C. Bleek, *Global Cleanout: An Emerging Approach to the Civil Nuclear Material Threat* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2004; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/bleekglobalcleanout.pdf as of 13 April 2005).

[2] "Fact Sheet: Project Vinca" (Washington, D.C.: U.S. Department of State, 23 August 2002; available at http://www.state.gov/r/pa/prs/ps/2002/12962.htm as of 28 September 2005).

[3] The NRC physical protection regulations are in U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials," in *Title 10, Code of Federal Regulations* (Washington, D.C.: U.S. Government Printing Office; available at http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html as of 28 September 2005). Section 73.6(e) exempts special nuclear material at all "non-power reactors" from nearly all of NRC's physical protection requirements. The very modest remaining requirements that research reactors with 5 kilograms or more of U-235 in HEU must meet can be found at Section 73.60. Research reactors are exempt from even these requirements if the U-235 is in irradiated fuel emitting more than 100 rem per hour at 3 feet – a level of radiation that is not remotely sufficient to deter suicidal terrorists, as discussed later in this chapter.

[4] Both the evolving DOE rules and the international rules on categorization of nuclear material are discussed extensively in this chapter.

In short, the problem of how to assess which materials, at which facilities, pose the most urgent dangers of nuclear theft remains one where there is little consensus and much inconsistency. Remarkably, it appears that neither the U.S. government nor the IAEA yet has a prioritized list assessing which facilities around the world pose the most serious risks of nuclear theft – that is, a list that integrates assessments of factors such as the quantity and quality of material at each site (and therefore the chance that adversaries could make a nuclear bomb from it), the security at that site, and the level of capability adversaries might be able to bring to bear for a theft attempt in the area where the site exists. But in a world of limited resources – not only of money but of the time and attention of senior officials and the political capital needed to convince facilities and countries to cooperate – it is crucial to develop such an assessment of the highest priorities to be addressed. While no single government or international organization can control nuclear security worldwide, considerable efforts are being invested in reducing the risks of nuclear theft (by the United States, the IAEA, and other governments), and it is clearly important to ensure that those investments are targeted on reducing the highest risks. Indeed, in the immediate aftermath of the 9/11 attacks, IAEA Director-General Mohammed ElBaradei identified such a prioritization as *the* most urgent step the world community needed to take: "the most immediate task is to achieve a more complete picture of nuclear security worldwide, to enable a rapid response to the most urgent needs, and to develop a coherent plan for longer term action."[5] This chapter provides a systematic risk-based method for developing such an assessment of "the most urgent needs."

Past assessments of these issues have generally focused on qualitative descriptions of how "easy" or "difficult" it would be, for example, to make a bomb from particular types of materials;[6] similarly, they have typically focused on some particular level of adversary capability as the maximum "credible," and estimated risk reduction by estimating decreases in the ability of that specified level of capability to succeed, rather than treating adversary capabilities as a continuous spectrum with some probability of capabilities above and below the specified level. (The question that might be asked in these types of studies might be "how much would the proposed upgrade reduce the probability that 3-5 well-armed attackers in league with one well-placed insider would be able to steal material from this facility?"[7]) The

---

[5] L. Wedekind, "Upgrading Nuclear Security Tops Board Agenda" (Vienna: International Atomic Energy Agency, 1 February 2002; available at http://www.iaea.org/NewsCenter/News/2002/01022002_news01.shtml as of 4 October 2005).

[6] See, for example, U.S. National Academy of Sciences, Panel on Reactor-Related Options, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options* (Washington, D.C.: National Academy Press, 1995; available at http://books.nap.edu/html/plutonium/0309051452.pdf as of 30 December 2006). This study gives 1-5 ratings for the quality of different types of nuclear material, but makes no attempt to convert those ratings into estimates of the risk posed by such materials.

[7] This is the general approach to vulnerability assessment at nuclear sites in the United States, based on a fixed "design basis threat" (DBT) that facilities are required to defend against. For a study that is particularly explicit in describing a reduction in the chance that one particular DBT could steal material as a reduction in the overall risk, see William C. Brundson, "Nuclear Terrorism Risk Reduction: Evaluating the Effectiveness of the Department of Energy's United States/Russian Nuclear Material Protection, Control, and Accounting (MPC&A) Program" (Ph.D. dissertation, Graduate School of International Studies, University of Denver, 2005). In this chapter, I use the notion of the level of "adversary capability" and the level of "threat" more or less interchangeably, much as the term "threat" is used in the phrase "design basis threat."

approach taken in this chapter, by contrast, is explicitly based on quantitative estimates of probabilities and risks, much like probabilistic risk assessment (PRA) for nuclear safety. (Indeed, offering a method that is explicitly based on thinking about adversary capabilities as a probability distribution, rather than a fixed maximum credible threat, is one of the major contributions of this chapter.)

There is an obvious problem with applying this approach to security, which is the difficulty of assessing the probability of various actions by intelligent adversaries who can change their tactics and develop their capabilities in response to defensive measures that may be put in place. In the case of safety, it is possible to collect historical data on matters such as the probability of earthquakes of varying magnitudes, or the rate of occurrence of various types of human errors, and base future predictions on this past experience, because no one is consciously *trying* to increase the chance that the system will fail. Estimating the probability of types of events that have never occurred before is an obvious problem, but there is usually at least some historical data on which judgments can be based. In the case of security, by contrast, adversaries *are* trying to make the system fail and will presumably change their approaches in order to increase their chance of success. For the risk analyst, thinking through all the varieties of creative malevolence adversaries might come up with is a difficult problem, and the types of actions adversaries have taken before is a less reliable guide to the likelihood that they will do so in the future. On September 10, 2001, very few people would have said that an attack involving four well-trained teams of 4-5 dedicated, suicidal individuals each, hijacking four separate airliners at approximately the same time with no prior warning and using them to kill thousands of people was a threat with a high enough probability to be worth worrying about very much.

Nevertheless, judgments about whether to invest more to protect a particular type of material or not, or whether to put higher priority on upgrading security at one facility rather than another, are inevitably based on judgments about relative risks – either implicit or explicit. The method described in this chapter helps structure thinking – and may help highlight important risks that have so far been ignored – by making these implicit judgments explicit.

Estimating the *absolute magnitude* of the risk of nuclear theft at any given facility or transport leg is effectively impossible, given the immense uncertainties in essentially all of the relevant parameters.[8] There is more hope of developing reasonable estimates of *relative* risks

[8] Attempts to estimate the absolute magnitude of terrorism risks posed by individual facilities can create dangerously misleading results – especially if they simply assume that the future will be the same as the past. In one recent study by the Electric Power Research Institute (EPRI), for example, commissioned by the Nuclear Energy Institute (NEI), the authors argued that even though they estimated a 35% chance that an attack by terrorist saboteurs on a U.S. nuclear plant would be successful in defeating the plant's defenses, the risk to the public from possible terrorist attacks on U.S. reactors was nevertheless negligibly small. This was because (a) terrorists would probably not attack (such attacks were estimated as having an average frequency of once every 2,500 years!), and (b) terrorists would probably be too incompetent to cause a major release even if they did attack and did succeed in overcoming the plant's defenses (assessed as only 1% chance of a major release). As it is impossible to calculate either of these probabilities, the study's conclusion that the risk is extremely low has no defensible basis. Doug True et al., *Risk Characterization of the Potential Consequences of an Armed Terrorist Ground Attack on a U.S. Nuclear Power Plant* (Palo Alto, Cal.: Electric Power Research Institute,

– that is, whether one facility poses more or less risk than another. Even in that case, the large uncertainties in estimating the probability that potential adversaries will attempt, or be able, to carry out various tasks – such as chemically processing uranium-aluminum research reactor fuel to recover uranium metal, to take just one example – means that any estimation of relative nuclear theft risks, even one informed by all available classified information, will inevitably contain a large element of technical judgment. Estimates of some of the parameters are, in effect, educated guesses. There is room for honest disagreement over the relative difficulty of various possible routes terrorists might take to the bomb – and therefore over the relative risks posed by different materials at different facilities. Nevertheless, current national and international rules and recommendations calling for "graded safeguards," which call for materials that would be easier to use to construct a nuclear explosive to receive higher levels of security, are inevitably based on such judgments about the relative difficulty of different paths to the bomb.

In this chapter, I will present a number of key judgments on these matters. Each of these judgments is subject to debate, but by presenting a systematic framework for analysis, I hope to provide a structure that will make it possible for participants in such a debate to identify specifically where they differ, discuss the reasons for their varying perspectives, and ultimately narrow their differences. The approach draws very directly on the risk model presented in Chapter 3, focusing on how different aspects of the security level for facilities and transport legs around the world, the spectrum of adversary capabilities that might be involved in theft attempts at these facilities and transport legs, and the quantity and quality of nuclear material affect the probability of successful theft and the probability of subsequent successful bomb-making.

Because of the complexities and uncertainties that make it impossible to make absolute estimates of risk – or even indisputable relative rankings of risk among different facilities – regulations and other policies relating to nuclear security should be "risk-informed," taking insights from attempts to explicitly estimate risks of different facilities into account along with other means of making judgments about priorities, rather than "risk-based," relying only on quantitative risk calculations. Such a mix of explicit probabilistic risk analysis and technical judgment is generally also the best practice with respect to safety of highly complex systems.[9]

In this chapter, I will proceed as follows. First, I describe the factors that determine the risk of nuclear theft from particular facilities and transport legs, offering an example involving two hypothetical countries with different risk profiles to be assessed. Second, I examine the spectrum of plausible capabilities and characteristics that nuclear thieves might

---

2003; available at http://www.nei.org/documents/EPRINuclearPlantConsequencesStudy20032.pdf as of 26 September 2005). Only the Executive Summary of this report has been made publicly available, and therefore the reasoning behind these remarkable conclusions is not provided.

[9] George E. Apostolakis, "How Useful Is Quantitative Risk Assessment?" *Risk Analysis* 24, no. 3 (2004). For a discussion of this problem as it relates specifically to physical protection vulnerability assessment, see Matthew Bunn, "Systems Approaches to Security for Nuclear Materials and Facilities", Presentation, "Research Seminar in Engineering Systems," Massachusetts Institute of Technology (Cambridge, Mass.: Managing the Atom Project, Harvard University, 4 December 2001).

bring to bear in attempting to carry out a theft. Third, I describe how different types of information about the potential adversary capabilities in different countries might be used to inform assessments concerning the probability that nuclear thieves would have various levels of capability in different countries. Fourth, I describe how other categories of information could be used to judge the effectiveness of nuclear security systems at different facilities and transport legs in defeating these various potential levels of adversary capability. Fifth, I examine the spectrum of plausible capabilities that the recipients of a stolen nuclear weapon or stolen nuclear material might bring to bear for the task of turning the stolen items into a usable nuclear explosive capability. Sixth, I provide an extended discussion of current approaches to categorizing what types of nuclear material require what levels of security; after examining how a wide range of barriers posed by the physical form of material that might be stolen (including isotopic, radiological, chemical, and size and mass barriers, among others) would affect the odds that different types of adversaries would be able to gain a usable nuclear explosive capability from them, I propose a new approach to categorizing nuclear materials for nuclear security purposes. A briefer discussion of the potential usability of stolen nuclear weapons with different characteristics follows that discussion of materials. I then summarize the risk assessment method developed in the chapter and provide an example, applying two different approaches to the method to a set of example countries to assess the nuclear theft risks there. Finally, I discuss how opportunity can be integrated with risk in assigning priorities, so that reductions in nuclear risk that can be achieved easily can be addressed quickly even if they are not the highest-risk sites.

The Factors That Determine Theft Risk

The risk of any event is the probability of that event multiplied by its consequences. Hence even low-probability events may pose high risks if their consequences are catastrophically high, as would be the case if terrorists were to get and use a nuclear bomb.

The risk of nuclear theft from any particular facility or transport leg, R, is the probability that a theft attempt will occur there, P_{at}, multiplied by the probability that such an attempt would be successful, $P_{s(at)}$, multiplied by the consequences of theft of the particular types of weapons or materials present at that facility, C:

$$R = P_{at} P_{s(at)} C$$

This approach is effectively identical to the risk equation used in assessing physical protection measures at DOE sites.[10]

---

[10] This approach is effectively identical to the "risk equation" used in assessing physical protection measures at DOE sites, where the probability of successful theft is expressed as one minus the probability that the security system would be effective in defeating the attempt, or 1-P_E:

$$R = P_{at}(1 - P_E)C$$

See, for example, Byron Gardner, "Process of System Design and Analysis," paper presented at Workshop on Physical Protection, Moscow, 11-14 September 1995 (available at http://www.osti.gov/bridge/servlets/purl/112931-7hNczP/webviewable/112931.pdf as of 9 January 2007). This approach is valid even though P_{at} and $P_{s(at)}$ are not likely to be independent (the probablity of a theft attempt is presumably higher at facilities where adversaries judge the probability of the attempt being successful to be higher). In essence, $P_{s(at)}$ is a conditional

What factors affect the terms in this equation? As outlined in Chapter 3, the probability that a nuclear theft attempt would be successful, $P_{s(at)}$, is, in essence, the probability that the capability that the thieves manage to bring to bear turns out to be more than the security system for that facility or transport leg can defeat. Hence, the *security level* for a particular facility or transport leg and the level of *adversary capability* that thieves might be able to bring to bear in a particular country or region are the first-order terms in estimating the probability that a theft attempt would be successful.[11]

The potential consequences, should nuclear theft occur, are the possibility that this would lead to either a proliferating state or a terrorist group gaining a nuclear explosive capability that they would not otherwise have acquired – or sooner than they otherwise would have acquired it. The ultimate consequence might well be the detonation of a nuclear bomb in a major city, with the loss of tens or hundreds of thousands of lives, hundreds of billions to trillions of dollars in economic damage, and far-reaching social and political effects. In this chapter, rather than repeating the very rough estimates of the magnitude of these consequences from Chapter 3, I will use the probability that adversaries would be able to transform the stolen items into at least one substantial-yield nuclear explosive capability, P_w, as an indicator of the consequences of theft from any given facility, so an adjusted risk factor, R_a, would be given by:

$$R_a = P_{at} P_{s(at)} P_w$$

This is a simplification of the reality. It assumes, in effect, that the consequences of *any* substantial-yield terrorist nuclear bomb are so immense that one should not focus unduly on the additional consequences if the yield were very large (as might be the case if terrorists managed to detonate a stolen weapon from the arsenal of a major state, rather than making a crude bomb of their own from stolen nuclear material), or if the terrorists managed to detonate two, or five, or ten weapons. Obviously the consequences in those cases *would* be higher – and in a worst case, one might imagine a breakpoint where nearly infinite consequences

---

probability, the probability that an attempt would be successful given the circumstance that an attempt has occurred – and therefore its influence on the chance that a theft would occur does not affect the validity of the approach.

It is easy to show that any or all of these factors can be normalized (so that some particular value corresponds to a particular chosen number, such as 1.0) by multiplying both sides of the equation by a constant, without affecting the resulting relative risk rankings between different facilities and transport legs. Later in this chapter, for example, I will introduce a "discount factor" describing the difficulty of making a nuclear bomb from the stolen items, where the most attractive materials (actual nuclear weapons, or large quantities of HEU metal) will have discount factors of 1.0, and all other materials will have discount factors somewhere between 0 and 1.0.

[11] Certain aspects of what has been called the "environment" at the nuclear facility – such as whether large quantities of material are being processed by hand on a regular basis, at one extreme, or all the material is always locked in a vault to which almost no one has access, on the other extreme – also affect the probability of theft. As discussed later in this chapter, these elements of the "environment" can usually be included in assessments either of the security level at a facility or transport leg, or of the insider threat there. For a discussion of this "environment" factor, see J.P. Hinton et al., *Proliferation Vulnerability Red Team Report*, SAND97-8203 (Albuquerque, N.M.: Sandia National Laboratories, 1996; available at http://www.osti.gov/bridge/servlets/purl/437625-gCUCGr/webviewable/437625.pdf as of 14 August October 2006).

would ensue, if terrorists managed to get a number of nuclear weapons sufficient to effectively cause a major state to collapse as a functioning society.[12]

Equally clearly, however, the difference between zero terrorist nuclear weapons and one is a gigantic, yawning gap: any effective policy to reduce the risk of nuclear terrorism must ensure that any facility or transport leg with even one weapon, or one bomb's worth of nuclear material, is secure enough to reduce the risk it poses to a low level. Hence, that is what the method proposed here focuses on. This simplification has only a modest effect on the recommended policies resulting from the analysis, as stringent security measures are clearly needed at any site with one nuclear weapon or the material to make one, and it is difficult to make the case that security measures should be dramatically different for a site with enough material for two or three bombs. (This is also implicitly the approach taken in existing U.S. and international nuclear security rules, where all sites with enough attractive nuclear material for even one improvised nuclear device require very high levels of protection, and sites with enough material for more devices do not require more.) If after providing stringent security measures for sites with one nuclear weapon or the material to make one, policy-makers choose to put in place even more stringent security measures for sites with somewhat larger numbers of weapons or somewhat more material, there is no reason to challenge this choice; but it should be seen as an additional measure once the urgent task of providing effective security for all the facilities and transport legs with at least one nuclear bomb or its essential ingredients has been addressed. (Indeed, as discussed in more detail in a later section, because of the possibility of accumulating material from more than one theft, even sites with only half or a quarter of the material needed for a nuclear bomb require significant security measures.)

The factors that determine P_w, the probability that a nuclear theft will lead to the recipients of the stolen items gaining a usable nuclear explosive capability vary depending on whether it is nuclear weapons or weapons-usable nuclear materials that have been stolen. As discussed later in this chapter, in the case of a stolen nuclear weapon, this probability is determined by the capabilities of the recipient group and by the efficacy of the safeguards incorporated into the weapon (for those attempting to set the weapon off) or the quantity and type of nuclear material inside the weapon (for those who might attempt to mine the weapon for nuclear material to make a bomb). In the case of stolen nuclear material, the probability that the recipients would be able to make a bomb from it is determined by their capabilities and by the quantity and quality of the nuclear material they receive – issues discussed in considerable detail in later sections.

The probability that a nuclear theft attempt will occur at a particular facility or transport leg is affected by the same factors that affect the other two terms: that probability will be higher for a facility or transport leg in an area with higher potential adversary capabilities (e.g., higher in Pakistan than in Canada); it will be higher for facilities with

[12] I am grateful to John P. Holdren for emphasizing this point. For a critique of the simplification used here, emphasizing that there would be large differences in the number of deaths and the quantity of economic damage between small terrorist nuclear blasts and very large ones, see Michael Levi, *On Nuclear Terrorism* (Cambridge, Mass.: Harvard University Press, 2007).

weaker security, where adversaries would likely judge they had a better chance of carrying out a theft successfully; and it will be higher for facilities with weapons or materials that would give the recipients a better chance of achieving their goal of a usable nuclear explosive capability. (Non-rational factors, such as how famous a particular facility may be, or how closely linked it may be to some controversial military activity, may also factor into thieves' decisions concerning where to make a theft attempt, but these are difficult to predict in advance, and are therefore difficult to include in assessments of the relative risk posed by different facilities or transport legs.)

Hence, in assessing which facilities pose the largest risks of nuclear theft, the most critical factors are:

1. the security level for the facility or transport leg (that is, what types of adversaries the security in place is able to defeat);
2. the likely distribution of capabilities of insider and outsider adversaries where the facility or transport leg in question is located;
3. the quantity of weapons-usable nuclear material available to be stolen (and in particular whether there is enough for a crude terrorist bomb); and
4. the quality of the material or warheads that might be stolen (that is, how difficult to overcome are the *barriers* to making a bomb created by the form of the material, whether these are created by its mass and bulk, its radioactivity, its chemical form, or its isotopic composition, or to detonating the weapon posed by the type of safeguards with which the weapon is equipped).

An Illustration: Nuclear Theft Risks in Two Hypothetical Countries

As an illustration of how factors such as security level, adversary capability level, and quantity and quality of material might interact to affect the overall risk of nuclear theft, consider two hypothetical countries. (The numbers used in this example are purely illustrative; in the real world, it would be very difficult to assess either the spectrum of adversary capabilities or the capability of security systems to defeat them so precisely.) Each country has only one facility with weapons-usable nuclear material. Country A has relatively low outsider and insider threats, while Country B faces higher potential adversary capabilities – as might be evidenced, for example, by the scale and frequency of terrorist attacks or insider theft conspiracies that take place there. (Indicators that might be used to assess these various factors are discussed in more detail later in this chapter.) Because of the higher threat it faces and various other bureaucratic and political drivers, Country B has more substantial security measures in place at its nuclear facility. But the quantity and quality of the material at Country A's facility is better, making it easier to make a nuclear bomb from material stolen from the facility in Country A. If one divides the various plausible levels of adversary capability into bins, each with an estimated probability that a theft attempt would have a capability in that range and each with an estimated probability that the security system in place would be able to defeat a capability in that range (rather than the more conceptual continuous distribution of threats and security levels from Chapter 3), the situation might appear roughly as shown in Table 4.1. (In this table, probabilities in the column "Attempt

Table 4.1: The Risk of Nuclear Theft in Two Hypothetical Countries

	Country A		Country B	
Threat Level	Attempt prob. at this level	Success prob. at this level	Attempt prob. at this level	Success prob. at this level
Beyond design threats	0.01	1.0	0.05	1.0
10-15 well-armed outsiders, and/or 1-4 insiders	0.09	0.95	0.15	0.7
4-9 well-armed outsiders, and/or 1-2 insiders	0.3	0.7	0.4	0.4
1-3 well-armed outsiders, and/or 1 insider	0.5	0.2	0.3	0.05
1 unarmed outsider, or 1 poorly placed insider	0.1	0.05	0.1	0.0
Prob. theft attempt is successful		0.41		0.33
Prob. of theft attempt		0.1		0.2
Prob. of bomb-making		0.4		0.2
Probability of theft + bomb-making		**0.0164**		**0.0132**

prob. at this level" are the probabilities *if* a theft attempt actually occurs, and sum to one; the resulting probability that a theft attempt would be successful if it occurred is then multiplied by the probability of such an attempt occurring at all, and the probability that the items stolen in a successful theft could successfully be made into bomb to find an overall probability of theft and bomb-making.)

As can be seen, the facilities in Country A are only well-protected (that is, the probability of successful theft is low) in the case of modest adversary capabilities, but large groups of attackers or insider conspiracies of several well-placed individuals would be almost certain to succeed in stealing nuclear material from its facility. Country B's more substantial security systems offer almost complete protection against modest adversary capabilities, and some significant chance of defeating even the larger capabilities. (In both cases, though, adversaries with capabilities well beyond those envisioned in the security system's design would be essentially certain to succeed in defeating the security systems.) Overall, Country B faces a roughly 50% higher chance that a successful theft will occur, despite its more effective security arrangements, because of the higher chance that a theft attempt will occur in Country B and the higher chance that if an attempt does occur, it will include a more capable set of adversaries. But because the material in Country A would be easier to use to make a nuclear bomb – giving the adversaries twice as high a likelihood of succeeding in that step, compared to the material in Country B – the facility in Country A poses a higher overall risk than the

facility in Country B, despite the much smaller chance of a theft attempt and the less capable likely adversaries in Country A.[13]

Most policy-makers, before having gone through an analysis of this kind, might assume that facilities in countries like Country A – which might correspond, for example, to countries like Japan or Belgium – pose little risk, compared to countries facing higher terrorist threats and higher dangers of insider theft conspiracies. That may indeed be the case, depending on just how different the probabilities of various types of theft attempt are; but it would be unwise to assume that the danger of nuclear theft in countries such as Japan and Belgium is acceptably low until analysis has supported that conclusion.

The remainder of this chapter will discuss each of these factors in turn, assessing their effect on overall risk. The chapter will then examine U.S. and international approaches to categorizing which quantities and qualities of material require what levels of security and propose a modified approach.

Preference vs. Probability

The approach in this chapter focuses on risk – the probability that an item could be stolen and the probability that such a theft would result in terrorists gaining a usable nuclear weapons capability. Issues such as the number of person-hours of work required to process the stolen material into a bomb, or the quantity of acid needed to dissolve the material, may strongly affect which materials terrorists would *prefer* to have, but may have only modest effects on the probability that adversaries will succeed in turning the stolen materials into a usable bomb before they are stopped. In an extreme case, a material modification that would impose more work on potential terrorists who received such stolen material but would not reduce their chances of success in that work would not significantly reduce the risk of nuclear terrorism; hence, to keep risk at an acceptable level, the modified material would require the same level of protection as unmodified material would.

The Probabilistic Spectrum of Capabilities of Plausible Thieves

Both the probability of nuclear theft and the probability that theft would lead to a usable nuclear capability depend crucially on the capabilities and tactics of the potential adversaries in question. It is useful, in thinking about the kinds of capabilities that matter, to divide the potential adversaries into *thieves* (those who carry out the actual theft of the nuclear weapon or nuclear material) and *recipients* (those who may receive the stolen items and ultimately attempt to get a usable nuclear explosive out of them). While both of these stages of the operation might be carried out by the same group (or different parts of the same adversary network), they involve quite different capabilities.[14]

---

[13] Note that, because nuclear material is so readily transportable, the variance in adversary capabilities from one country to another should be considered in assessing the probability of the initial theft, but should not be a major factor in considering the consequences of that theft. Just because the terrorists in a particular country were considered incapable of making a bomb would not mean that a theft of HEU in that country would have no substantial consequences, as the bomb-making may be done by others, in other countries.

[14] In most cases, in addition to the original theft and the processing of the material into a usable nuclear explosive, there would also be transport of the material from the theft site to another site suitable for the

Before discussing approaches to assessing threat levels, security levels, and the environment at different types of nuclear facilities, it is worth briefly discussing the spectrum of plausible capabilities that thieves might bring to bear to steal nuclear weapons or materials. As already noted (and discussed in Chapter 3), potential thieves may have a broad range of different levels of capability – and for many facilities and transport legs, equipped with substantial security systems, only the highest-capability thieves are likely to have any significant probability of successfully stealing a nuclear bomb or enough material to make one. (Later, before discussing different quantities and qualities of nuclear material, there will be a similar brief discussion of the spectrum of plausible capabilities of potential recipients.)

There are limits to the threat any nuclear security system can handle. No plausible nuclear security system will protect nuclear warheads or materials from theft by a rogue division of armed troops or by a conspiracy of all the top management of the facility where these items reside. At the opposite end of the spectrum, security systems involving only modest cost and inconvenience can prevent theft by a single outsider or a single poorly placed insider. Between these extremes, nuclear security systems incorporating more or less stringent measures would have different probabilities of successfully stopping a theft attempt. Individuals or groups who might try to steal a nuclear weapon or nuclear material fall on a probabilistic spectrum of capabilities, which probably includes many potential thieves with only modest capabilities (who could be deterred or defeated by relatively modest nuclear security measures) and fewer and fewer groups having the needed capabilities as the task becomes more difficult.

Conceptualizing the problem of the range of different capabilities thieves might have as a spectrum of greater or lesser capability – an essentially one-dimensional concept – is itself a substantial simplification, as thieves' characteristics may vary across several dimensions, and different security systems may be better designed to handle one type of adversary strength than another. A site with highly trained access controllers with a questioning attitude may be well-equipped to defeat thieves planning to rely on deception (for example, wearing official uniforms and using forged official IDs to attempt to enter), while another site whose guards are heavily armed and trained in tactical response may be better equipped for defeating adversaries planning to rely on a frontal attack. Some of the obvious potential variations in the characteristics of plausible thieves are discussed below.

As discussed in Chapter 3, one key distinction in describing the types of plausible theft threats is between thefts by insiders (people with authorized access to the facility and its material, possibly with detailed knowledge of the facility's security system and its weaknesses), by outsiders without such authorized access, or by both insiders and outsiders working together. Typically a conspiracy of both insiders and outsiders is the most difficult

---

manufacture of the bomb, and possibly transport of the bomb to the target. Additional groups may be involved in this chain, and the stolen items may conceivably pass through several sets of hands between thieves and recipients. But because the essential ingredients of a nuclear bomb are small and difficult to detect, and hence relatively easy to transport and smuggle across national borders, the most important adversary capabilities in determining the overall risk are likely to be those of the thieves and the recipients, and hence they will be the focus in this chapter.

threat for a physical protection system to defend against, particularly if it includes multiple insiders.

Another important distinction is whether the theft is to be *covert* (done in the hope of keeping the effort a secret, at least until after the nuclear material has been removed), or *overt,* that is, done with no attempt to hide the fact that a theft was underway (typically by force). A typical example of an overt, forcible theft would be an armed robbery at a bank. From the thieves' point of view, there are immense advantages to a covert theft; in the case an overt theft, even if it is successful in getting a weapon or material out of the facility, the thieves will have to cope with nearly immediate response and pursuit.[15] Appropriate use of security cameras and other monitoring mechanisms, however, can make it very difficult for a theft attempt to remain covert – though not impossible (as evidenced by the Antwerp Diamond Center heist discussed below, among other cases). Ensuring that any removal of a nuclear weapon or material will be detected immediately, so that a theft could not remain covert, is an important minimum objective of a nuclear security system.

Those instigating a theft, whether insiders or outsiders, might fall into several categories, with quite different typical characteristics:

- **Opportunists**. These are people who steal when they see an opportunity to do so, but may not have any sophisticated theft plan and probably have little willingness to kill or risk their own lives in carrying out their theft. They may also have no particular plan for selling the material when they carry out the theft. This category has accounted for essentially all of the thefts of HEU and plutonium whose details have been confirmed to date.
- **Professional criminals**. Professional criminals, particularly if linked to substantial organized crime groups, might bring more planning, larger numbers, more willingness to use violence, and more capable armament and equipment to the job than opportunists would. They would presumably be stealing the material to sell it to some one else, since there is absolutely no credible evidence that professional criminals have been seeking nuclear weapon capabilities of their own (though a variety of blackmail scenarios can be imagined). As professionals, in the business to make money, they presumably would not carry out suicidal attacks. Professional criminals might be outsiders or might infiltrate a targeted facility and become insiders. Professional criminals might also *instigate* the

[15] The one circumstance in which this may not be a major concern to the thieves is the situation in which their plan is to attempt to rapidly assemble and detonate an improvised nuclear device while they are still within the facility – or detonate a weapon present within the facility. For facilities that contain assembled nuclear weapons or nuclear materials that offer the possibility of such rapid assembly into a crude device, DOE security rules require that the defense plan to keep attackers out of the facility entirely, rather than being based, for example, on trapping them within the facility after they have broken in. See, for example, discussion in U.S. Congress, Government Accountability Office, *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat* (GAO, 200423 December 2006). Building and detonating a crude device, or detonating a stolen weapon, within minutes or hours, using only materials and equipment the thieves brought along or could find at the site, is plausible for certain types of nuclear material, but would clearly be more difficult than making or detonating a bomb if the adversaries were able to transport the stolen items to a secret location where they could work on the problem for months or years.

theft, without being the ones to carry it out themselves – for example by bribing or blackmailing insiders to carry out the theft. To date, there is little substantial evidence of organized crime involvement in the known nuclear theft attempts, but this always remains a possibility.

- **Terrorists**. Like professional criminals, terrorist groups presumably could bring a substantial level of planning, armament and violence to bear on committing a theft of nuclear material. A terrorist group might be stealing material for itself, or for transfer to another group or state with which they were linked. (An obvious possibility of that kind is theft by Chechen terrorists for transfer to al Qaeda; some of the more extreme Chechen factions have had close links with al Qaeda.) Unlike professional criminals, terrorists might well be willing to carry out attacks in which their own death is accepted as part of the plan, as was the case in the 9/11 attacks. Like criminals, terrorists could be outsiders or might succeed in becoming insiders, and they could carry out the theft themselves, or instigate others to do so. As discussed in Chapter 3, there are no documented cases of terrorists stealing nuclear weapons or materials, but there are worrisome suggestions that they might, such as the terrorist reconnaissance at Russian nuclear warhead sites in 2001. Russia's interior minister has confirmed that "international terrorists have planned attacks against nuclear and power industry installations... to seize nuclear materials and use them to build weapons of mass destruction."[16]
- **Agents of foreign powers**. Over the years, there have been concerns in a number of countries that teams working for a foreign state might attempt to steal a nuclear weapon or material, or sabotage a major nuclear facility. Such teams would presumably be primarily outsiders, but might succeed in infiltrating an insider into the targeted facility, or bribing or blackmailing an existing insider to help them. There is no published record of confirmed incidents involving teams of agents of foreign powers stealing nuclear weapons or fissile materials.
- **Protesters.** The only actual attempts to break through nuclear security systems that most guard forces ever see are by protesters. As a result, protesters have a significant impact on how nuclear security systems in many countries are structured and operated, though protesters would be highly unlikely to attempt to actually steal nuclear weapons or nuclear materials. In a few cases, protesters have been armed and used violence (as in the case of the rocket-propelled grenade fired at the French SuperPhenix reactor decades ago, for example).

Whatever the category of the potential thieves, the key question is what specific capabilities and tactics they are likely to bring to bear. Obviously, the more capable the group of thieves envisioned, the more capable the security system must be to have a high probability of defeating the adversaries. The United States and a number of other countries have in place regulatory systems under which each nuclear facility that falls in a particular defined class (such as a power reactor, or a facility with more than a specified amount of HEU) is required

[16] "Internal Troops to Make Russian State Facilities Less Vulnerable to Terrorists," *RIA-Novosti*, 5 October 2005.

to provide security designed to defeat a specified set of possible adversary capabilities, known as the "design basis threat" or DBT. The IAEA has recommended that all states with weapons-usable nuclear material or major nuclear facilities to protect have such a defined DBT as the basis for their physical protection approaches.[17] As noted in Chapter 3, the DBT approach effectively takes one particular point on the spectrum of possible adversary capabilities and describes that as the maximum credible threat that facilities are required to defend against, rather than attempting to assessing the probability distribution for different levels of adversary capability.[18]

What should be included in such DBTs? What adversary capabilities should facilities with nuclear weapons or weapons-usable nuclear materials be required to be able to defend against? This is inevitably a matter of balancing security and cost. On the one hand, it is important to be defended against obviously plausible threats, but on the other hand, it is important not to waste money defending against imagined armies of 10-foot-tall terrorists. The nuclear industry, which in most countries has to bear much of the cost of security at its facilities, would inevitably draw the balance at a different point than would those in the rest of society who bear many of the risks of failure but few of the costs of action; hence, it is the job of regulators to tug the balance to a point they judge to serve the broader interests of society.[19]

Some observers, noting that the vast majority of terrorist and criminal actions are carried out by small groups (or even single individuals) have argued that nuclear facilities need only be defended against small groups with limited capabilities. Taking this line of thinking, before 9/11, the U.S. NRC only required U.S. nuclear power plants to be protected against attack by a "small group," reportedly three outsiders, possibly in league with one insider;[20] the DBT for theft of HEU or plutonium was reportedly only modestly higher. Others have argued that typical terrorist assaults involve small numbers of people only

---

[17] International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected) (Vienna: IAEA, 1999; available at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html as of 22 December 2006).

[18] In some countries, there is a clear acknowledgment that the DBT facilities are required to defend against is *not* the maximum credible threat, but only the maximum threat that the security systems at individual sites are charged with coping with. In the United States, for example, the Atomic Energy Act specifies that the federal government, not individual licensees, is responsible for providing defense against enemies of the state. The NRC has interpreted this to mean that licensees should only be responsible for defending against relatively modest threats; there do not, however, appear to be specific procedures in place for the federal government to fulfill its responsibility to defend against more substantial threats, if a theft attempt begins before intelligence has detected the conspiracy unfolding. For discussion, see Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, *Nuclear Security: Has the NRC Strengthened Facility Standards since 9/11?* U.S. House of Representatives, 109th Congress, 2nd Session, 4 April 2006 (available at http://reform.house.gov/NSETIR/Hearings/EventSingle.aspx?EventID=41937 as of 6 May 2006).

[19] Whether the government or privately owned hazardous facilities (such as nuclear facilities) should pay the costs of increased security, and in what proportion, is a difficult question that is not addressed in this dissertation. An argument can be made for the government paying for the societal benefit of reducing the security externalities posed by such facilities, but an argument can also be made for a principle similar to "polluter pays."

[20] See, for example, Daniel Hirsch, "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.thebulletin.org/article.php?art_ofn=jf02hirsch as of 8 January 2007), pp. 38-44.

because that is what the perpetrators "perceived to be necessary to accomplish their mission," and that such small numbers do "not represent an upper limit on their capacity to mobilize people."[21] Indeed, an examination of terrorist attacks and crimes involving high-value, guarded non-nuclear targets over the past two decades demonstrates the remarkable range of outsider and insider threats that terrorists and criminals have demonstrated they are able to pose.[22]

Large overt attack. Terrorists have repeatedly demonstrated the ability to mount large overt armed attacks. In September, 2004, for example, 34 heavily armed terrorists seized a school in Beslan, starting a hostage crisis that ended in a massacre in which hundreds were killed, most of them children. In October 2002, 41 heavily armed, well-trained, suicidal Chechen terrorists (the 19 women in the group all had explosives attached to their bodies) struck a Moscow theater in a carefully planned attack launched without warning, seizing hundreds of hostages.[23] The official Russian government newspaper reported that the group had considered seizing facilities at Moscow's Kurchatov Institute (where hundreds of kilograms of highly enriched uranium, enough for dozens of nuclear weapons, is located).[24] Large overt attacks have occurred in a number of other countries as well. The 9/11 attacks themselves involved 19 well-trained terrorists.

Multiple coordinated teams. The 9/11 attacks provided an especially clear example of the use of multiple, independent, well-coordinated teams striking simultaneously. These attacks involved four teams, each with four to five well-trained, suicidal participants, from a larger organization with access to heavy weapons and explosives. The groups spent over a year collecting intelligence and planning, yet succeeded in striking without warning without the conspiracy being detected in advance. Many nuclear facilities today have security systems designed only to handle a single team of attackers. Multiple teams of attackers can significantly complicate the defense: one team, for example, might distract the defenders while the real attack was carried out by another, or one team might be assigned to mine the road to prevent response forces from arriving to defeat the team carrying out the actual theft.

Significant covert attack. Criminals often use covert outsider or insider attacks to strike their target without the defense even being aware until after the crime has been committed. On February 16, 2003, for example, sophisticated thieves stole an estimated $100 million in gems from 123 vaults in the Antwerp Diamond Center, one of the most secure jewel-handling facilities in the world. The thieves, while outsiders, apparently had extensive

---

[21] Brian Michael Jenkins and Joseph L. Krofcheck, "Appendix III-A: The Potential Nuclear Non-State Adversary," in *Nuclear Proliferation and Safeguards* (Washington, D.C.: Office of Technology Assessment, 1977). These authors provide an exceptionally thoughtful discussion of some of the issues discussed in this section.

[22] For earlier examples of a similar approach to assessing the threat, see Bruce Hoffman et al., *Insider Crime: The Threat to Nuclear Facilities and Programs*, R-3782-DOE (Santa Monica, Cal.: RAND, 1990); Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, N-1498-SL (Santa Monica, Cal.: RAND, 1980).

[23] For a description, see, for example, "118 Hostages Are Dead in Moscow Theater Raid," *The Russia Journal*, 27 October 2002.

[24] Vladimir Bogdanov, "Propusk K Beogolovkam Nashli U Terrorista (a Pass to Warheads Found on a Terrorist)," *Rossiskaya Gazeta*, 1 November 2002.

insider knowledge of the security system and were able to overcome security cameras, an alarm system, and more to keep their theft undetected until the following day, when they were long gone.[25] In Brazil in 2005, a sophisticated gang of thieves spent three months digging a roughly 80-meter tunnel under the heart of the town of Fortaleza, coming up into a bank vault without detection and making off with an estimated $67.8 million.[26] In a similar nuclear-related case in India in 2003, thieves reportedly drilled through a wall to avoid a sophisticated alarm system at the front gates, in order to steal three canisters containing cobalt-60.[27]

Use of deception and diversion. Criminals have frequently used deception to trick their way through a target's defenses. In 1990, for example, thieves dressed as policemen tricked the guard at the Gardner Museum in Boston into letting them go into the museum and remove several priceless works of art, including a Rembrandt.[28] In 2002, Chechen fighters wore Russian military uniforms and used forged official passes to get a truck filled with explosives through three successive military checkpoints, in a suicide truck-bombing that destroyed the headquarters of Chechnya's Russian-backed government and killed at least 72 people.[29]

Intelligence collection, planning, and acquisition of specialized skills. Both terrorists and criminals have demonstrated an ability to collect information about potential targets and plan their attacks on them over extended periods of time. The 9/11 attacks involved well over a year of detailed collection of intelligence on U.S. airline schedules, security procedures, and other factors. The Antwerp Diamond Center heist appears to have involved at least three years of planning and intelligence collection. In the case of the 9/11 attacks, the terrorists trained as pilots in order to carry out the attack, consciously acquiring a specialized skill for a hostile purpose. In the case of the Antwerp Diamond Center, investigators believe an Italian criminal group known as the "School of Turin," including criminals with specialties in skills such as safe-cracking and defeating alarm systems carried out the theft. In many cases the intelligence collection includes successfully gaining access to inside information, not available to the general public. The Antwerp Diamond Center thieves clearly had detailed knowledge of the design of the security system – including the fact that a key to the vault was, inexplicably, stored right next to the vault and how the alarm system could be prevented from going off.[30]

---

[25] See, for example, "The Great Diamond Heist," "PrimeTime Live," *ABC News*, 12 February 2005; Chris Summers, "Hopes of Finding Diamond Haul Fade," *BBC News Online*, 14 February 2004 (available at http://news.bbc.co.uk/1/hi/world/europe/3364911.stm as of 22 December 2005).

[26] Stan Lehman, "In Brazil: Thieves Tunnel into Bank Vault for $67.8 Million," *Associated Press*, 10 August 2005.

[27] "Radioactive Material Stolen from Steel Plant in Eastern India," *Associated Press Newswires*, 17 August 2003.

[28] Elizabeth Neuffer, "Gardner: Masterwork of Crime: Retracing the Steps of Robbery's Twisted Trail," *Boston Globe*, 13 May 1990. For other examples of the common deception tactic, see Reinstedt and Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs.*

[29] Guy Chazan, "Chechens Turn on Each Other -- after Years of Attacking Russians, Local 'Collaborators' Are New Foe," *Wall Street Journal*, 30 December 2002.

[30] "The Great Diamond Heist."

Use of heavy weapons and sophisticated explosives. Automatic weapons such as the ubiquitous AK-47 are widely available to terrorist and criminal groups all over the world. Rocket-propelled grenades (RPGs) are also available worldwide. Such weapons have been used frequently in Chechen terrorist attacks and in attacks in Iraq and elsewhere. Highly accurate long-range armor-piercing weapons (such as .50-caliber armor-piercing rounds) can, unfortunately, be purchased at gun shows and other venues in the United States. RPGs and large-caliber armor-piercing rounds can be devastatingly effective against body armor and armored fighting positions for guards at facilities – though relatively low-cost means are available to counter such adversary weaponry.[31] Similarly, from the attack on the *USS Cole* to ongoing attacks in Iraq, terrorists have repeatedly demonstrated an ability to use increasingly sophisticated explosives – and attackers who know what they are doing can use explosives to breach both fences and concrete walls remarkably quickly.[32] Indeed, Al Qaeda training videos show terrorists training in the use of explosives such as platter charges to blow through security doors.[33]

Use of unusual vehicles. Criminal groups have frequently used a variety of vehicles to help them get through security systems. For example, helicopters have been used in many recent prison escapes.[34] In the United States, the Department of Homeland Security's *National Planning Scenarios* – the set of attacks and disasters the United States should be prepared to cope with – assumes that attackers could easily rent helicopters for use in their attacks.[35] Similarly, the six men convicted for planning a heist of $500 million worth of diamonds from London's Millennium Dome in November 2000 used a bulldozer to break into the dome, then planned on using a speedboat along the Thames to escape.[36] The security plans at many nuclear facilities are not designed to cope with attackers arriving and departing in a helicopter or speedboat.

Theft of material in transit. When valuable materials – whether diamonds or nuclear weapons – are being moved from place to place, it is impossible to have the same layers of security that can be provided at a fixed site with walls, fences, vaults, and other fixed barriers. In countries around the world, thefts of hundreds of thousands to millions of dollars from armored cars equipped with armed guards happen every year. Indeed, in France, robberies of armored cars by "very well-organized...paramilitary-type" gangs, using "Kalishnikovs, bazookas, and bombs" became so frequent that in May 2000 the armored car drivers went on strike, demanding hazard pay and an end to night transports.[37] Yet an analysis of extensive

---

[31] "Systems under Fire," *U.S. Department of Energy, Office of Independent Oversight and Performance Assurance*, 2003.
[32] "Systems under Fire."
[33] "Systems under Fire."
[34] See, for example, "5 Use Copter to Break out of Prison," *Los Angeles Times*, 31 December 2002; John Tagliabue, "Latest in a Series of Bold Breaks Frees 3 Inmates at French Jail," *New York Times*, 15 April 2003.
[35] *National Planning Scenarios* (Washington, D.C.: U.S. Department of Homeland Security, 2005; available at http://media.washingtonpost.com/wp-srv/nation/nationalsecurity/earlywarning/NationalPlanningScenariosApril2005.pdf as of 4 October 2005), pp. 6-2.
[36] Sue Leeman, "Scotland Yard Foils Huge Jewel Heist," *Associated Press*, 8 November 2000.
[37] See, for example, Anne Swardson, "Armored Car Driver Strike Shortchanges Parisians; Atms Empty While Merchants Are Flush," *Washington Post*, 16 May 2000.

photographs taken of French transports of separated plutonium – which occur roughly weekly – suggests that these transports would be dangerously vulnerable to similar types of attacks.[38]

Use of insiders. Terrorists and criminals around the world frequently use insiders and insider information. Insiders may be motivated by sheer desperation for money, as appears to have been the case with the 1992 theft of 1.5 kilograms of 90% enriched HEU from the Luch facility in Russia, for example.[39] Insiders may simply be greedy, as is the case with countless crimes around the world.[40] Insiders may be vengeful and disgruntled. In one case in the early 1990s, for example, a group of six employees at a Halliburton facility in India admitted to stealing three radioactive sources and dumping them in a nearby river, simply because they were angry over a decision to transfer one of the six to another site.[41] Disgruntled ex-employees, who are familiar with the location of valuable items and the facility's security system and may still have good contacts among current employees, have also played a key role in many major crimes.[42] Insiders may also be ideologically motivated – as in the case of senior Pakistani nuclear weapon scientist and Islamic extremist Sultan Bashiruddin Mahmood, an anti-American Islamic extremist who after his retirement met with Osama bin Laden and discussed nuclear weapons at length.[43]

Many nuclear facilities have programs to limit access to employees who have been screened for trustworthiness, to address these kinds of insider problems. But even if all the insiders are believed to be highly reliable, they might be coerced into joining a scheme against their wishes. In a case in Northern Ireland in 2004, for example, thieves apparently linked to the Provisional Irish Republican Army (IRA) made off with £26 million from the Northern Bank. While the bank's security system was designed so that only two managers of the bank together could open the vault, the thieves kidnapped the families of two bank managers and blackmailed them into helping the thieves carry out the crime.[44] (The thieves also used deception in this case, appearing at the bank managers' homes dressed as policemen.) One of these managers, however, has now been charged with participating voluntarily in the crime;

---

[38] Ronald E. Timm, *Security Assessment Report for Plutonium Transport in France* (Paris: Greenpeace International, 2005; available at http://greenpeace.datapps.com/stop-plutonium/en/TimmReportV5.pdf as of 6 December 2005). While this analysis was prepared for Greenpeace, Timm is a well-known security analyst who spent decades doing vulnerability assessments and physical protection designs for DOE facilities. This analysis provides a useful comparison of the conditions shown in the photographs Greenpeace collected to the security approaches required for comparable nuclear materials transported by DOE.

[39] See, for example, the interview with Yuri Smirnov, the convicted perpetrator, in "Frontline: Loose Nukes: Interviews" (Public Broadcasting System, 1996; available at http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/ as of 22 December 2005).

[40] Hoffman et al., *Insider Crime: The Threat to Nuclear Facilities and Programs.*

[41] "Radioactive Device Stolen from Halliburton India Unit," *Dow Jones Newswires*, 11 October 1993.

[42] Reinstedt and Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs.*

[43] For the Mahmood case, see, for example, David Albright and Holly Higgins, "A Bomb for the Ummah," *Bulletin of the Atomic Scientists* 59, no. 2 (March/April 2003; available at http://www.thebulletin.org/issues/2003/ma03/ma03albright.html as of 2 January 2007), pp. 49-55; Peter Baker, "Pakistani Scientist Who Met Bin Laden Failed Polygraphs, Renewing Suspicions," *Washington Post*, 3 March 2002.

[44] For a good introduction to the Northern Bank case, see Chris Moore, "Anatomy of a £26.5 Million Heist," *Sunday Life*, 21 May 2006.

he denies the charge.[45] If in fact it is the case that these managers only participated because their families were held hostage, no personnel reliability program in the world would have turned them up as security risks, suggesting that other measures also need to be taken to guard against insider threats. Kidnapping to blackmail family members into carrying out certain actions has been a common Chechen terrorist tactic.[46] Such tactics are frequently successful.[47]

Insiders may be in any position – including senior managers and also guards. (In one database, guards were responsible for 41% of insider thefts at guarded facilities.[48]) There may be more than one insider, as in the Northern Bank case: conspiracies of multiple insiders, familiar with the weaknesses of the security system (and in some cases including guards or managers) are among the most difficult threats for security systems to defeat. Yet insider conspiracies are relatively common. In 1998, for example, an insider conspiracy at one of Russia's largest nuclear weapons facilities attempted to steal 18.5 kilograms of HEU—potentially enough for a bomb.[49] And, of course, insiders can collude with outsiders, playing roles ranging from simply providing information, to disabling critical security systems, to using armed violence to help the outsiders attain their objectives.[50]

These are not James Bond fantasies from Hollywood. These are real events that have occurred in the last couple of decades. These examples are deeply sobering, documenting the broad range of capabilities that terrorists and criminals have succeeded in bringing to bear to carry out thefts and attacks. It would be politically, though not technically, impossible to ensure that every facility in the world where a nuclear weapon or the material to make one existed had a security system as strong as the one at the Antwerp Diamond Center – yet that system was defeated. This highlights the fact that improved security measures can only reduce the risk of theft, never eliminate it; the danger that nuclear material could be stolen from a particular building can be eliminated only by removing the material, so that there is nothing there to steal.

A strong case can be made that nuclear weapons and their essential ingredients should be defended at least against the kinds of capabilities that terrorists and criminals have demonstrated in real incidents (especially incidents that occurred in the country or region where the particular nuclear cache in question is located). Some would go further and argue

---

[45] Moore, "Anatomy of a £26.5 Million Heist."
[46] Robyn Dixon, "Chechnya's Grimmest Industry: Thousands of People Have Been Abducted by the War-Torn Republic's Kidnapping Machine," *Los Angeles Times*, 18 September 2000.
[47] Reinstedt and Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs.*
[48] Hoffman et al., *Insider Crime: The Threat to Nuclear Facilities and Programs.*
[49] This attempt was first officially revealed by the Russian Federal Security Service (FSB), who claimed credit for foiling it. See Yevgeniy Tkachenko, "FSB Agents Prevent Theft of Nuclear Materials," *ITAR-TASS*, 18 December 1998. The attempt was discussed somewhat more by Victor Erastov, chief of material accounting for what was then Russia's Ministry of Atomic Energy. See"Interview: Victor Yerastov: Minatom Has All Conditions for Providing Safety and Security of Nuclear Material," *Yaderny Kontrol Digest* 5, no. 1 (Winter 2000). Neither of those accounts identified the type of material; that is from an interview by the author with a Ministry of Atomic Energy official, 2000.
[50] For a discussion of crimes of this type, see Hoffman et al., *Insider Crime: The Threat to Nuclear Facilities and Programs.*

that nuclear weapons and the materials to make them should also be defended against capabilities that are not yet demonstrated, but easily imaginable. On the other hand: (a) criminals with the most extensive capabilities have generally focused their efforts on theft of items such as cash and jewels, which are relatively easily turned into untraceable money (though jewels often pose a problem in that respect), raising the question of what the probability is that comparable capabilities would be applied to stealing nuclear weapons or materials; (b) none of the cases described above involve *all* of the capabilities just described being brought to bear at once, raising the question of what fraction of these capabilities nuclear facilities should be required to be able to defend against in a single attack; and (c) in nearly all the cases just described, some or all of the criminals or terrorists involved were eventually caught. If a nuclear weapon or the nuclear materials to make one were found to be missing, the effort invested to catch the perpetrators and recover the stolen goods would presumably be far greater; that factor might well deter some groups, if they concluded that they would not have a good enough chance of both carrying out the theft and avoiding capture for long enough to make effective use of the stolen nuclear goods.

Resources for nuclear security are inevitably limited. Providing reliable protection against the kinds of threats just described requires, in effect, a military level of security, even at civilian sites, which in itself raises troubling issues. Clearly, not all of these possible adversary capabilities are equally likely. There are probably large numbers of potential opportunistic insiders in the world who might take advantage of a gaping security weakness to steal nuclear material, but who could be deterred from doing so by even fairly rudimentary security systems. The chance of a large-scale military-style attack with multiple teams aided by knowledgeable insiders is obviously far lower.

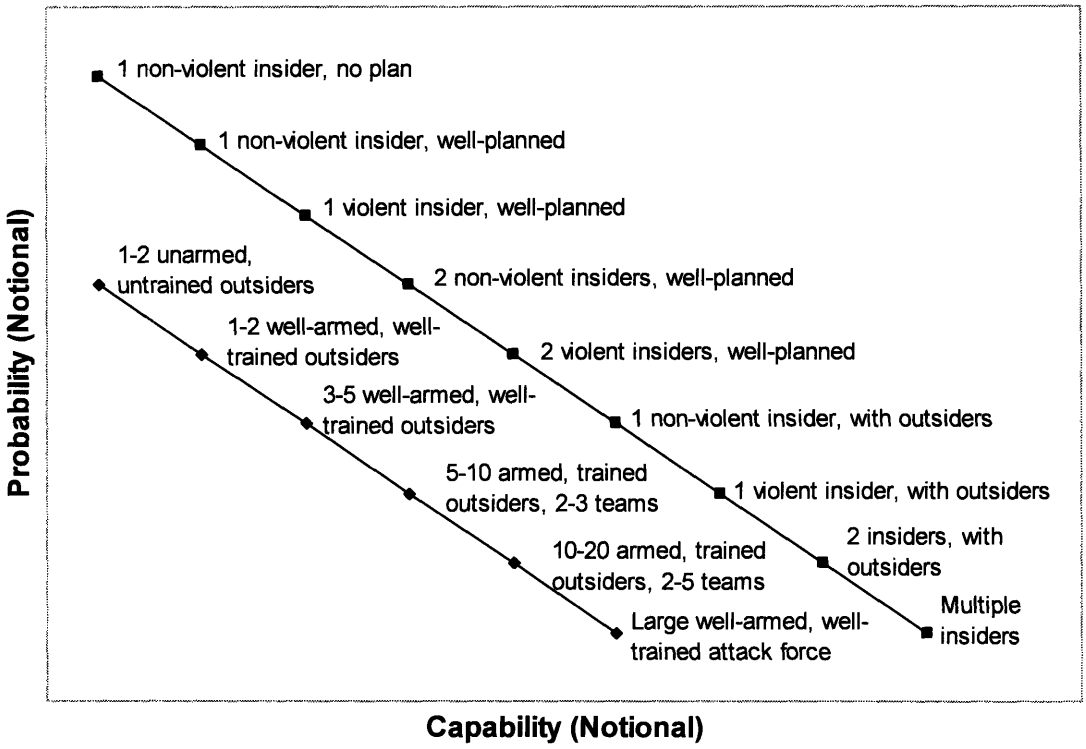
An illustrative version of the spectrum of capabilities of plausible thieves is shown in Figure 4.1. The placement of many of the points on this graph could be debated (are multiple insiders more or less likely than two insiders working with outsiders, for example); it is intended primarily as a basis for thought and discussion. The placement of the insider and outsider lines on the chart is intended only to get both on one chart, not to imply that outside attackers are always less probable than insiders. Much of the debate over what nuclear facilities should be required to defend against boils down to a debate over what the shape of this chart really looks like – and in particular, how low the probability of a theft attempt by adversaries with substantial and sophisticated capabilities really is.

Assessing the Threats Adversaries Pose at Different Facilities

While terrorists have demonstrated global reach in some cases, there is little doubt that the level of capability adversaries could plausibly bring to bear to attempt to carry out a nuclear theft varies from one country to the next and within particular areas of some countries. A nuclear security system that might be perfectly adequate in Canada might not be sufficient in Pakistan, and one that might be adequate in St. Petersburg might not be enough in Chechnya.[51]

[51] All nuclear weapons had been removed from the Caucasus republics of the former Soviet Union before the Soviet Union collapsed. There are no known facilities with separated plutonium or HEU in Chechnya or nearby

Figure 4.1: The Probabilistic Spectrum of Plausible Thieves



Given this combination of global threat with local variations, a prioritized risk-minimization strategy would seek to ensure that all facilities with nuclear weapons, separated plutonium, or HEU worldwide are effectively protected against a common minimum threat and that those facilities facing higher threats are provided an appropriately higher level of security.

---

areas of Russia, either. There were previously two sites with HEU in Georgia, but the HEU from one of these sites was airlifted to Britain in Operation Auburn Endeavor in 1998, while the modest amount of HEU from the other site, at Sukhumi, remains missing. For a discussion of Auburn Endeavor, see Thomas A. Shelton et al., "Multilateral Nonproliferation Cooperation: US - Led Effort to Remove HEU/LEU Fresh and Spent Fuel from the Republic of Georgia to Dounreay, Scotland (Auburn Endeavor/Project Olympus)," in *Proceedings of the 21st International Meeting on Reduced Enrichment for Research and Test Reactors (RERTR), Sao Paulo, Brazil, 18-23 October 1998* (Argonne, Ill.: Argonne National Laboratory, 1998; available at http://www.rertr.anl.gov/Fuels98/SpentFuel/SThomas.pdf as of 2 December 2006). For the Sukhumi incident, see "Confirmed Proliferation-Significant Incidents of Fissile Material Trafficking in the Newly Independent States (NIS), 1991-2001" (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 30 November 2001; available at http://cns.miis.edu/pubs/reports/traff.htm as of 3 March 2006). Substantial quantities of radiological material suitable for use in a "dirty bomb" are still located in Chechnya, however, particularly at a site of the Russian radioactive waste management organization Radon, located near Grozny, which has repeatedly been the target of thieves. See, for example, Yuri Bagrov, "Cache of Unprotected Radioactive Material Found in Chechnya," *Associated Press*, 16 April 2003; Amina Bisaeva, "Chechnya's Ticking Radiation Bomb," *Environment News Service*, 27 January 2005 (available at http://www.ens-newswire.com/ens/jan2005/2005-01-27-01.asp as of 2 December 2006).

A wide variety of sources of information are available to judge the level of different types of threats in different countries and different areas of them. First and foremost, the analysis should include an assessment of real incidents (both nuclear and non-nuclear) that have occurred in recent years in the country or area in question and what they may indicate about the capabilities adversaries can bring to bear. Have there been large overt armed attacks? How large, with what weapons and tactics? Have there been insider theft conspiracies? How sophisticated were they?

A variety of factors have to be taken into account in considering how much weight to give to different types of incidents. Obviously attacking a nuclear facility in an attempt to steal nuclear material is a very different thing from attacking an undefended school, as terrorists did at Beslan in 2004. But the fact that terrorists were able to bring to bear 34 heavily armed attackers, willing to die, and were able to strike without warning without being detected in advance by the police or intelligence services, is nonetheless quite relevant in assessing what types of outsider attacks on nuclear facilities are plausible and have to be taken into account in planning defenses of those sites. Overall, the frequency in any given country or area of those types of crimes that are most relevant to nuclear theft should be a key factor in assessing the threat. These include terrorist attacks (both outsider attacks and attacks involving insiders); insider theft of high-value items; and outsider thefts of high-value items (including both overt and covert thefts, and thefts both from fixed facilities and from transports, such as armored cars).

Besides actual incidents, several other factors should be taken into account, including:

- levels of presence and activity of both terrorist groups and organized crime groups;
- actions or statements by these groups indicating an interest in acquiring nuclear weapons or materials;
- levels of corruption and insider theft, in the society at large and among the staff and guards of nuclear facilities in particular;
- levels of pay and morale among nuclear staff and guards;
- facility or transport leg location (e.g., in a major city or a remote area, how effectively is the area nearby monitored for unusual activities, how close are major roads or other means adversaries might use to arrive and depart, etc.);
- record of the police and intelligence services in detecting and stopping high-capability conspiracies before they can achieve their objectives; and
- measures for screening and monitoring nuclear staff and guards for trustworthiness.

Where possible, facility-by-facility information on such factors should be collected (and regularly updated);[52] where such facility-specific information is not available, at least

[52] For a brief summary of early results of a research project focusing on corruption, theft, organized crime, and extremism in and around the Russian closed nuclear city of Ozersk (home of the Mayak Production Association, one of Russia's largest plutonium and HEUsites), see Robert Orttung and Louise Shelley, *Linkages between Terrorist and Organized Crime Groups in Nuclear Smuggling: A Case Study of Chelyabinsk Oblast*, PONARS

national-level information should be collected. French government researchers have recommended a similar approach to assessing insider threats, emphasizing the need to "gather on the ground information on the potential threat," including both "conditions inside the facility" related to worker morale and human reliability programs and "conditions outside the facility," such as the presence of organized crime or terror groups.[53]

Fortunately, nuclear security analysts do not have to start from scratch in preparing these kinds of assessments. The insurance industry routinely makes detailed estimates of the risks of different types of theft or terrorist attack in different countries, in order to be able to judge the price they should charge for insurance coverage against such threats. Since large profits or losses ride on these estimates, they are likely to be higher quality than many government assessments. Most of this analysis is proprietary, but would be readily available to governments willing to purchase it. Some assessments of overall threat levels made on behalf of the insurance industry are publicly available. One consulting firm, for example, publishes a global index ranking 186 countries on the basis of their estimate of the terrorism risk in those countries.[54] Transparency International publishes international rankings of perceptions of the level of corruption in different countries;[55] other organizations also publish global corruption estimates, such as the rankings on "control of corruption" included in the governance data published by the World Bank.[56] Where information on how much nuclear staff and guards are paid is not available, gross domestic product per capita (adjusted for purchasing power parity) could provide a rough indicator of whether pay levels (and the resources available for other nuclear security investments) are likely to be high or low. This is a very rough indicator, however, as employees at some types of nuclear facilities (such as nuclear weapons programs in countries where those programs are considered essential to state survival) may get pay substantially above the national average, while employees at other types of facilities (such as civilian research reactors in countries where science receives few resources) may get below-average pay; and research in behavioral economics suggests that above some subsistence level of income, *relative* income – whether conditions are worse than before, or worse than those of others in the country in question – may be more important in determining attitudes than absolute income.[57]

Once nuclear security analysts have compiled these types of information, they then have to analyze it to make judgments about the probability that adversaries could bring

---

Policy Memo No. 392 (Washington, D.C.: 2005; available at http://www.csis.org/media/csis/pubs/pm_0392.pdf as of 12 April 2006).

[53] C. Brouse et al., "IRSN Activities in Physical Protection in Support of the IAEA: The Insider Threats Approach," in *Eurosafe Forum 2003: Paris, 25-26 November* (Paris: Eurosafe Forum, 2003; available at http://www.eurosafe-forum.org/products/data/5/pe_190_24_1_5_9paper.pdf as of 30 July 2006).

[54] Guy Dunn, *WMRC Global Terrorism Index 2003/2004* (London: World Markets Research Centre, 2003).

[55] See, for example, Transparency International, *Corruption Perceptions Index 2004* (Berlin: TI, 2004; available at http://www.transparency.org/content/download/1532/7971/file/media_pack_en.pdf as of 16 November 2006).

[56] See Daniel Kaufmann, Aart Kraay, and Massimo Mastruzzi, *Governance Matters IV: Governance Indicators for 1996-2004* (Washington, D.C.: World Bank, 2005; available at http://www.worldbank.org/wbi/governance/pdf/GovMatters_IV_main.pdf as of 1 August 2006).

[57] Andrew E. Clark and Andrew J Oswald, "Satisfaction and Comparison Income," *Journal of Public Economics* 61, no. 3 (September 1996).

different levels of outsider or insider capability to bear to steal nuclear weapons or materials in a particular country, or from a particular facility or transport leg. Such judgments will always be difficult and controversial. But making them is the second essential step in estimating the probability that, in any particular nuclear theft attempt, adversaries will be able to bring to bear a level of capability sufficient to defeat the security system and carry out a successful theft.

The Facility Environment's Contribution to the Threat

In addition to the factors just described, certain elements of what has been termed the "environment" at a nuclear facility are important to judging the scale of the insider and outsider threats the facility might face.[58] Many elements that could be considered as the "environment" should be included in assessments of the levels of security at different facilities, such as whether the material at a facility is stored in a locked and monitored vault, whether two-person or three-person rule is enforced whenever anyone accesses the material, how people are screened to determine their trustworthiness, and the like. But other important elements of the facility environment that could affect the magnitude of the insider and outsider theft threats may not be included in standard security system assessments. These might include, among others:

- The number of people with authorized access to the material in question (if only a few people have access, the insider threat will likely be easier to control);
- Whether the material at the facility is only being stored unused, or is being regularly handled and processed (especially if it is being processed in bulk, offering more opportunities for removing small amounts without detection);
- Whether the quantity of material needed for a bomb would be almost all of the material at the facility (and hence difficult to remove without detection), a tiny fraction of the material at the facility (possibly easier to remove without detection), or in between;
- Whether the material at the site is in large heavy forms that are easy to count and difficult to remove covertly (such as assembled nuclear weapons or fuel assemblies) or in powders or small pieces that can easily be carried off in secret.

Nuclear security analysts should ensure that each important element of the environment is integrated either into the assessment of the security level at the facility or transport leg or into the assessment of the threat adversaries may be able to pose to it.

Assessing the Threats Security Systems Can Defeat

To assess the risk of nuclear theft posed by a particular facility or transport leg, assessing the capabilities of its security system is an essential step. This assessment should be threat-based – that is, what levels of adversary capability, both outsider and insider, overt and covert, could the security system in question defeat, with what probability?

---

[58] For a report using this formulation in its assessments of the security of various types of operations, see Hinton et al., *Proliferation Vulnerability Red Team Report.*

The information available for making such an assessment and the resulting level of detail and confidence that it will be possible to have in the assessment, will vary dramatically depending on where the particular nuclear facility or transport leg is located. For an organization assessing security at its own facilities, detailed vulnerability assessments can be performed, which seek to assess what pathways into the facility for theft or sabotage would be most likely to be successful, how long the delays for the adversary would be for each of the necessary steps the adversary would have to take along those pathways, what the probabilities for the defender to detect and correctly assess the adversary would be at each of those steps, how effective on-site guards would be in defeating the adversaries, how long it would take off-site response forces to arrive, and how effective they would be in defeating the adversaries. In the U.S. Department of Energy (DOE) for example, such vulnerability assessments are routinely required for all nuclear facilities. Such vulnerability assessments make use of expert judgment; a variety of computer software packages, from the simple (and simplistic) Estimate of Adversary Sequence Interruption (EASI) to the more complex and realistic Analytic System and Software for Evaluating Safeguards and Security (ASSESS); and "tabletop" simulations of how adversaries might attempt to steal material or sabotage facilities and how defenders might react.[59] They are typically supplemented (and input data for such models collected) with various types of performance tests, ranging up to what are known as "force-on-force exercises," where "red teams" portraying adversaries attempt to break into a facility and defender teams attempt to stop them (along with similar tests involving insider threats).

Such methods provide invaluable information and are, today, the best that can be done to estimate the probability that a particular security system will be able to defeat a particular set of adversaries. But they are inevitably imperfect. Security planners may not envision every tactic that adversaries might think of to defeat a security system, possibly leaving defenses weak against some potential tactics; they may not envision (and tests may not reveal) all the things that may go wrong for the defense (including confused, frightened, or inebriated guards), especially as tests inevitably have an element of lack of realism, with the guards warned ahead of time concerning when the test will occur and using laser-tag equipment or other fake weapons rather than real weapons (so as to avoid testers actually being shot); and in complex tightly-coupled systems of this kind, it is inevitably difficult to foresee all the system interactions that may take place.[60]

In any case, such in-depth vulnerability assessments and tests are difficult to apply internationally, as many countries will not permit representatives from other countries to carry out such assessments and tests for their nuclear facilities, considering such information to be secret. Similarly, many countries are not likely to provide detailed accounts of the results of their own nuclear security assessments and tests. Countries vary in their willingness to provide other information that may contribute to assessing nuclear security levels. Some developing or transition states with only civilian facilities are happy to have international

[59] For an overview of vulnerability assessment and physical protection system design, see, for example, Mary Lynn Garcia, *The Design and Evaluation of Physical Protection Systems* (Woburn, Mass.: Butterworth-Heineman, 2001).

[60] For a critique of such methods making these points, see Bunn, "Systems Approaches to Security".

reviews of security at their facilities and international assistance in improving it; at the other end of the spectrum, a state like Israel, to take one example, which does not even acknowledge the existence of its nuclear weapons, is highly unlikely to provide any information whatever that would contribute to judging how well they are secured. Alliance relationships contribute to information-sharing in many cases – but critical nuclear security information is often not exchanged even between close allies.

As discussed in Chapter 3, the few nuclear facilities and transport legs with the weakest security systems are likely to pose a large fraction of the total risk of nuclear theft. Hence, whether there are some particularly vulnerable facilities within a particular country is even more important than what the *average* level of security for nuclear facilities and transport legs in that country may be. As a result, information on how rigorous a particular country's approaches to regulating and inspecting nuclear security are may be particularly important, as weak regulatory measures could allow some facilities to remain especially vulnerable for years or decades before regulators identified them and succeeded in getting their operators to take corrective action.

Several key sources of information are available that can inform relative judgments about nuclear security in different countries.

Intelligence information. Even for the United States, which may have the most extensive and expensive intelligence system in the world, information available on nuclear security from classified intelligence sources is quite limited. Satellite photographs of nuclear facilities can reveal some important factors, such as whether there are substantial fences with clear zones around a facility, whether armored personnel carriers are parked there, and whether vegetation has been allowed to grow up to or over the fences. But these images say nothing about whether the intrusion detectors are broken, whether the guards are patrolling with no ammunition in their guns, or whether the personnel at the facility are financially desperate or corrupt. Spies at these facilities, or interviews with employees who work there, can provide much more detailed information, and analysis of a variety of open sources can supplement such intelligence sources; but these sources require that the intelligence community be instructed to place high priority on collecting information on this subject, which has not yet occurred. In 1995, for example, the Joint Atomic Energy Intelligence Committee (JAEIC) prepared a highly classified assessment of nuclear security in the former Soviet Union, which concluded that not a single facility in the former Soviet Union had adequate safeguards and security to prevent nuclear theft.[61] Because at that time U.S. experts had only physically visited a few of these facilities, however, the actual information on security measures at these sites contained in this report was quite limited.

Technical cooperation. In some (but not all) cases, technical cooperation to improve nuclear security can include a wide range of visits and discussions that provide quite detailed

[61] This conclusion is mentioned, without specifically mentioning the JAEIC study, in the unclassified testimony of John Deutch, then Director of Central Intelligence, in Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction, Part II*, U.S. Senate, 104th Congress, 2nd Session, 13, 20, and 22 March 1996. At the time, I was directing a classified study of policy on improving nuclear security in the former Soviet Union, and had full access to relevant intelligence.

information on which to base judgments about the security of different facilities and transport legs. In the early days of U.S.-Russian cooperation on material protection, control, and accounting (MPC&A), Russia was unwilling to allow U.S. experts to visit *any* facilities that contained actual plutonium or HEU – even civilian facilities – judging the information about nuclear security that would be gleaned by such visits to be too sensitive. That sensitivity has long since been overcome, however, and a great deal of information has since been exchanged. Under current approaches, Russian experts perform vulnerability assessments of their own at facilities subject to cooperation and propose upgrades to correct weaknesses identified, with at least selected information from the vulnerability assessments to justify the proposals; U.S. teams work with them to develop a list of agreed upgrades; and Russian experts then implement the agreed upgrades, paid for with U.S. funds. U.S. experts are typically permitted to visit the facility once before upgrades begin, to confirm the need for them; once to assess the upgrade work while it is underway; and once to assess the completed upgrades. In many cases, a wide range of different types of upgrades may be implemented under several different contracts over a period of years, so the total number of visits may be substantially larger.[62] Although the United States does not get access to the detailed vulnerability assessments themselves, showing , for example, the easiest routes by which adversaries might be able to gain access to a particular facility, nonetheless the U.S. understanding of nuclear security in Russia has improved dramatically as this process has proceeded.

Such technical cooperation can lead to even higher levels of information exchange, or can keep virtually all information about nuclear security at particular sites protected. In the non-Russian states of the former Soviet Union, for example, in some cases facilities were willing to let U.S. analysts perform detailed vulnerability assessments and allowed U.S. groups to carry out "red team" tests of the security at the facility, providing even more detailed insight as to the real performance of the security systems at these sites than the United States has for Russian facilities.[63] By contrast, the cooperation with China has so far involved doing upgrades at only one facility, combined with intensive discussions of approaches China can use for finding and fixing vulnerabilities at its other facilities on its own.[64] Similarly, Pakistan has publicly acknowledged that it is cooperating with U.S. experts to improve security at Pakistani nuclear sites, but has said that this cooperation does not involve any U.S. access to Pakistani nuclear sites.[65]

In principle, the information developed as the result of such technical cooperation might be systematized, assessing performance of nuclear security systems in several different

---

[62] This process is described briefly in U.S. Department of Energy, *2006 Strategic Plan: Office of International Material Protection and Cooperation, National Nuclear Security Administration* (Washington, D.C.: DOE, 2006). See also Matthew Bunn, "Cooperation to Secure Nuclear Stockpiles: A Case of Constrained Innovation," *Innovations* 1, no. 1 (2006; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/INNOV0101_CooperationtoSecureNuclearStockpiles.pdf as of 4 April 2006).

[63] Interviews with U.S. participants in these assessments and tests, 1999-2000.

[64] Interview with DOE official, July 2006.

[65] Nirupama Subramanian, "Pakistan Accepted U.S. Help on N-Plants," *The Hindu*, 22 June 2006 (available at http://www.thehindu.com/2006/06/22/stories/2006062205201400.htm as of 28 July 2006).

categories (e.g., intrusion detection, alarm assessment, barriers and delays, protection forces, personnel reliability, access control, and so on) and then using weighting factors to come up with an overall assessment of performance that could be compared between sites. In the 1990s, for example, Lawrence Livermore National Laboratory in the United States developed a system in which U.S. teams working with individual sites in Russia would give the site they were working with ratings on a wide range of different areas of performance, which were then rolled into an overall 0-100 rating (with 100 the most secure) using weighting factors developed through polling of a group of U.S. experts. When this approach was tested on U.S. sites, where very detailed information was available, the typical rating was in the range of 70. This approach was never widely implemented, however.[66] Similarly, in the course of U.S.-Russian cooperation on improving nuclear security regulations in Russia, U.S. and Russian experts developed a set of roughly 350 key functional elements that regulations should require, in a prioritized list; that list, with appropriate weightings of the individual elements, could probably be adapted for use as a tool for assessing the state of nuclear security at particular sites.[67]

Information exchanges. Some international exchanges of information about nuclear security approaches and practices already take place, and such exchanges could be expanded in the future. The information exchanged in the context of U.S.-Russian technical cooperation, for example, has recently been expanded to include exchanges of "best practices" in nuclear security and accounting, including exchanges of experience in such matters as how best to draft and enforce nuclear security regulations.[68] A group of European nuclear security regulators meet regularly to discuss topics of mutual interest, which include experiences in implementing particular types of nuclear security regulations.[69] The United States already publishes information on the percentage of facilities of various types that have received high ratings, or have failed to do so, in security inspections and security tests.[70] It is easy to imagine that cooperating countries could work out arrangements under which they would describe to each other in detail the kinds of assessments, inspections, and tests that were done on their facilities and then provide summary-level information of this kind on the

---

[66] Personal communication from Deborah Yarsike Ball, Lawrence Livermore National Laboratory, 1999.

[67] Greg E. Davis et al., "Creating a Comprehensive, Efficient and Sustainable Nuclear Regulatory Structure: A Process Report from the U.S. Department of Energy's Material Protection, Control and Accounting Program," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).

[68] The first U.S.-Russian "best practices" workshop occurred in September 2005, with presentations on subjects ranging from nuclear security regulation to screening insiders for trustworthiness. (Data provided by both Russian and DOE officials.)

[69] This European Civil Nuclear Security Regulators Forum is mentioned briefly in Director of Civil Nuclear Security, *The State of Security in the Civil Nuclear Industry and the Effectiveness of Security Regulation: April 2002 – March 2003* (London: Office for Civil Nuclear Security, Department of Trade and Industry, 2003; available at http://www.dti.gov.uk/files/file23303.pdf?pubpdfdload=03%2F418 as of 28 July 2006).

[70] Indeed, changes in this percentage are used to track performance of the security program at the Department of Energy. See, for example, U.S. Department of Energy, *FY 2007 Congressional Budget Request: National Nuclear Security Administration--Defense Nuclear Nonproliferation*, vol. 1, DOE/CF-002 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_1_NNSA.pdf as of 3 January 2007), p. 418.

fraction of facilities that fared well or poorly in such reviews. Similarly, in the 1990s, a group at Stanford University, working with experts from several of the U.S. national laboratories, developed a detailed questionnaire on all aspects of MPC&A that could be filled out by the security managers at a facility; several facilities from different countries agreed to fill out all or a large part of the questionnaire.[71] One could easily imagine building a more widespread practice of voluntary sharing of data such as that included in the Stanford questionnaire. This kind of information exchange could help build confidence in nuclear security arrangements and provide additional information on which to base judgments about relative nuclear security levels in different countries.

International peer reviews. Both the IAEA and some individual states perform international peer reviews or overviews of nuclear security arrangements. Since the late 1970s, U.S. law has required that the United States review the adequacy of physical protection arrangements for U.S.-supplied nuclear material and facilities; U.S. experts have conducted some 145 physical protection reviews in more than 40 countries since then.[72] These visits tend to be relatively brief and the teams do *not* perform detailed vulnerability assessments of the facilities' ability to defend against particular design basis threats; rather, the teams review the regulations in place in a country and the security measures that exist at selected facilities to confirm that they are generally consistent with IAEA recommendations. While other members of the Nuclear Suppliers Group (NSG) also require recipients of their nuclear materials and technologies to provide at least a basic level of physical protection for them, it is not clear whether any of the other NSG members actually conduct on-the-ground reviews of recipients' compliance with these requirements. The IAEA began organizing international peer reviews of nuclear security, known as the International Physical Protection Advisory Service (IPPAS) in the mid-1990s.[73] The IAEA organizes an IPPAS review when a state requests such a review – so only states willing to have international experts see key aspects of their nuclear security systems end up being reviewed. In most cases, the review recipients have been developing or transition countries; in 2003, Norway became the first wealthy developed state to host an IPPAS review, sending the message that all countries can benefit from international review and advice.[74] Like the U.S.-led reviews, IPPAS reviews do not perform detailed vulnerability assessments or conduct tests of the actual performance of nuclear security systems in defeating particular types of threats; instead, they are focused only on confirming that facilities are generally following IAEA recommendations. Neither the U.S. reviews nor the IPPAS reviews make their conclusions public – both for the obvious reason of not revealing vulnerabilities to those who might want to exploit them, and because confidentiality encourages states to be willing to accept the reviews. Hence, in the case of the

---

[71] Personal communication from George Bunn, June 2005.

[72] Data provided by DOE, July 2006.

[73] For a brief description of IPPAS and its role, see Mark Soo Hoo, " IAEA Activities for the Physical Protection of Nuclear Material and Facilities -- the Role and Importance of IPPAS Missions," in *Eurosafe 2002, Berlin, 4-5 November 2002* (Berlin: Forum for Nuclear Safety, 2002; available at http://www.eurosafe-forum.org/products/data/5/pe_253_24_1_euro2_5_7_iaea_phys_pro.pdf as of 11 May 2006).

[74] Government of Norway, "Statement by Norway," in *48th IAEA General Conference, Vienna, Austria, 20-21 September 2004* (Vienna: International Atomic Energy Agency, 2004; available at http://www.iaea.org/About/Policy/GC/GC48/Statements/norway.pdf as of 10 May 2006).

U.S. reviews, only the U.S. government and the reviewed government receive the results (meaning that other governments or the IAEA could not use the data from these reviews to inform assessments of which facilities worldwide had what levels of security); in the case of the IPPAS reviews, only the IAEA, the reviewed government, and the participants on the review team are informed of the results of the review (similarly limiting the availability of the data to inform international assessments).

Laws, regulations, and other open sources. Many countries publish a considerable amount of information about their approaches to physical protection, including their laws and regulations on the subject (though some parts of these are often kept secret);[75] speeches and other statements on the subject by senior officials; and conference papers by their leading experts.[76] In countries with broad press freedoms, there is often additional information available in press reports about both strengths and weaknesses of approaches to nuclear security at particular sites. The United States makes more information publicly available than any other country and has particularly aggressive non-government organizations monitoring problems in U.S. nuclear security arrangements;[77] but important information about nuclear security in a variety of other countries can be gleaned from similar sources. In addition, in many cases it is possible to visit facilities and interview security experts and managers, collecting significant additional information that is not classified, but is not readily available to the general public. A number of important questions can often be answered through analysis of such open sources and compared across countries, such as: Does the country in question base its nuclear security rules on the IAEA recommendations? If so, which revision of the IAEA recommendations are the rules based on? (At this writing, the most recent version of INFCIRC/225 is Revision 4, completed in 1999; international discussions of a fifth revision are expected to begin in late 2006.) Does the country in question require its facilities with potential nuclear bomb material to be able to defend against a specific DBT? If so, is there any information at all in the public domain as to how substantial this DBT is? Does the country in question require facilities to have armed guards on-site at facilities with potential nuclear bomb material, or does it rely on armed response by forces that would have to come to the site from elsewhere in response to a call? (Tests in the United States have suggested that in some cases, if on-site defenses are defeated, either theft or sabotage might be accomplished quickly enough that off-site response forces might not have time to arrive.) Are nuclear material transports subject to similar requirements? What kind of screening is in

---

[75] The UN Security Council committee overseeing implementation of UN Security Council Resolution (UNSCR) 1540 has made a compilation of national laws on subjects covered by the resolution, including physical protection, available on their website. See United Nations, "1540 Committee" (New York: UN, 2005; available at http://disarmament2.un.org/Committee1540/meeting.html as of 25 February 2005).

[76] For selections of such papers, see, for example, Fritz Steinhausler, ed., *Proceedings of Strengthening Global Practices for Protecting Nuclear Material: Eu-High Level Scientific International Conference on Physical Protection, Salzburg, Austria, 8-13 September* (Salzburg, Austria: University of Salzburg, 2002; available at http://www.numat.at/list%20of%20papers/gesamtproceedings.pdf as of 4 December 2006); International Atomic Energy Agency, ed., *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations, Vienna, 10-14 November* (Vienna: IAEA, 1997).

[77] The work of the Project on Government Oversight is particularly notable in this respect. See, for example, Project on Government Oversight, *U.S. Nuclear Weapons Complex: Security at Risk* (Washington, D.C.: POGO, 2001; available at http://www.pogo.org/p/environment/eo-011003-nuclear.html as of 4 December 2006).

place to ensure that people granted access to nuclear material (or charged with responsibility for guarding it) are trustworthy?

Combined all-source analysis. Ideally, a full assessment of security levels at the many nuclear sites should be prepared which makes use of all the sources of information available. Unfortunately, as far as the author is aware, this has not been done – either in the United States, at the IAEA, or anywhere else in the world. After the 9/11 attacks, the United States did finally attempt to pull together information from various databases into a list of world facilities with HEU or plutonium. On this list, the analysts gave each facility that had been subject to a recent U.S. visit a one, two, or three rating for security, depending on whether it did not meet, just barely met, or clearly met the IAEA physical protection recommendations. In cases where the rating suggested a problem a few words were included to indicate what the problem was. But anyone wanting more detailed information – including information that might help inform an estimate of what kinds of threats a facility was defended against – would have to go back to the original trip reports of the visits. And information from the myriad other potential sources available was not integrated into this list.[78] As noted above, much more sophisticated methods for systematizing and weighting information about different elements of the overall effectiveness of nuclear security systems are available, if analysts chose to make use of them.

Using the information available within a government like the U.S. government or the Russian government (or at the IAEA, if adequate resources were available to undertake such an analysis), analysts could attempt to divide the security levels at different facilities and transport legs into bins, depending on the types of threats they were judged to be effectively protected against, much as in the example at the start of this chapter. For example, something like the following five-point scale might be used to rate facilities:

(1) Not well protected even against a single outsider or a single insider. (Some facilities in the former Soviet Union fell in this category in the early 1990s, as evidenced by successful thefts that involved only one insider or one outsider.)
(2) Probably protected against single outsiders, but likely still vulnerable to even a small group of determined outside attackers, or one to two well-placed insiders. (Many HEU-fueled research reactors around the world appear to be in this category; sites that followed the IAEA recommendations but went not further would probably be in this category or the next one.)
(3) Sites likely protected against one to three outside attackers, or one non-violent insider, but may still be vulnerable to well-planned attacks by a modestly larger group of well-armed, well-trained outsiders, one to three well-placed, determined, and violent insiders, or both working together.
(4) Sites probably protected against attacks by modest groups of outside attackers, one to three insiders, and both working together.
(5) Sites probably protected against squad-size force of well-trained and well-armed attackers, one to four well-placed insiders, and both working together. (Facilities

[78] Interview with DOE official, November 2005.

meeting the new DBT that DOE facilities are now required to protect against would be among the few facilities in the world protected at this level.)

As examples of such an approach, consider the nuclear facilities in the United States and Russia. Most DOE facilities are probably in the process of transition from category four to category five in this ranking system, as they put in place the measures needed to meet the new DOE DBT. Privately owned HEU facilities regulated by the NRC would be in category four, as they are not required to have defenses against the squad-size threats that DOE facilities are now required to protect against, or perhaps in transition between category three and category four. As already noted, however, HEU-fueled research reactors in the United States are exempt from the most important NRC security requirements for facilities with HEU, and most of them would likely be in category two. In Russia, it is highly unlikely that there are any longer any facilities in category one. Large weapons complex sites (comparable in some respects to the major DOE sites) are probably in category four for outside attackers, but in category two or three with respect to insider threats; small civilian sites are likely in category two or three with respect to both threats. (Ironically, after more than a decade of U.S.-Russian nuclear security cooperation, most HEU-fueled research reactors in Russia are probably better secured than their counterparts in the United States.)

Given the limits of available information on the real state of nuclear security at facilities around the world, such threat-based rankings will inevitably involve a certain amount of judgment and educated guesses – at any level of classification, in any government. Despite the uncertainties, however, an approach based on the threats analysts believe security systems can defeat is superior to approaches that are not threat based, because when it is combined with estimates of the probability that adversaries will bring particular levels of threat to bear, this approach can lead to a judgment concerning the probability of successful theft from a particular facility and how it compares to that probability at other facilities facing different levels of threat.

In short, making such estimates of the threats facilities can defend against is the first step in assessing the risks these facilities pose. The next step is assessing the kinds of capabilities adversaries might be able to bring to bear to challenge these security systems.

The Probabilistic Spectrum of Plausible Recipient Capabilities

Like potential thieves, potential recipients of stolen nuclear weapons or materials also fall on a probabilistic spectrum of capabilities, with many groups having at least modest capabilities and fewer and fewer groups having the needed capabilities as the task of using the stolen goods to gain a usable nuclear explosive capability becomes more difficult. Much of the task of assessing how much security different quantities and qualities of nuclear material require is based on attempting to judge what that probabilistic spectrum of adversary capabilities might look like – that is, what the probability of success would be, given different types of weapons and materials such a group might receive. The higher the probability the material in question could be made into a bomb, the higher the consequences would be of stealing that material and the more effort should be made to reduce the probability of its theft, in order to keep the conditional risk at an acceptable level.

Table 4.2: DOE Consequence Ratings for Different Materials

Material	DOE Consequence Ratings
Nuclear weapons	1.0
"Pure Products" Plutonium or HEU metal, Category 1 quantity	0.8
"Simple Compounds" Oxides, carbides, etc., Cat. 1 quantity	0.7
"High-Grade Material" Solutions, fuel assemblies, alloys, Cat. 1 quantity	0.6
Category 2 quantity or material	0.4
Category 3 quantity or material	0.2
Category 4 quantity or material	0.1

Source: Byron Gardner, "Process of System Design and Analysis," presented at "Workshop on Physical Protection," Moscow, 11-14 September 1995 (available at http://www.osti.gov/bridge/servlets/purl/112931-7hNczP/webviewable/112931.pdf as of 9 January 2007.

In this chapter, I do not attempt to assess the consequences of potential nuclear attacks in terms of lives lost and economic damage inflicted.[79] Since the goal of the analysis here is only to assess *relative* risks of nuclear theft – that is, which facilities pose larger risks than others – such an absolute assessment of consequences is not needed. Rather, in this chapter, the consequences assessment is based on judgments as to how the probability that recipients would succeed in getting a bomb that would detonate and provide a substantial yield from the stolen items varies depending on what the stolen items are. For different nuclear materials that might be stolen, I use a zero to 1.0 scale, with 1.0 assigned to large quantities of HEU metal (which, as discussed below, would be the easiest material in the world for terrorists to make a nuclear bomb with substantial yield from, as it could be used to make a simple but inefficient "gun-type" bomb, little more than slamming two masses of HEU together at sufficient speed). (Assembled nuclear weapons are discussed in a separate section below.) This 1.0 rating is only a relative judgment, not an absolute one: it says only that large quantities of HEU metal pose the greatest dangers, *not* that the probability that recipients would be able to make a bomb from a large quantity of HEU metal is anything like 100%. All other types of nuclear material are then assigned ratings based on judgments of how much lower the probability of recipients being able to make a bomb from them would be, compared to large quantities of HEU metal.

This approach is very similar to the approach DOE used for many years to assign consequence values in assessing the risks at different facilities. That consequence ranking

[79] For an official U.S. government analysis of the consequences of a 10-kiloton terrorist nuclear blast in Washington D.C. (remarkably leaving out entirely the effects of fire), see *National Planning Scenarios*. For an earlier analysis by the present author (along with John P. Holdren and Anthony Wier) of the effects of a 10-kiloton weapon detonated at Grand Central Station on a typical workday, see Matthew Bunn, Anthony Wier, and John Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/cnwm.pdf as of 2 January 2007), pp. 15-19.

also featured a zero to 1.0 scale, with the materials that would be easiest for terrorists to use in a nuclear bomb given the highest rankings and material that would be more difficult to process for use in a bomb given lower rankings. Table 4.2 shows DOE's consequences rankings for different types of materials as they existed in the mid-1990s.

How the quantity and quality of material that the recipients acquire affects the probability that they will be able to make a usable nuclear bomb from it depends on the recipients' capabilities. For example, some recipients might have experienced nuclear chemists and at least simple processing facilities available: the need to separate uranium or plutonium from other materials would pose a smaller barrier to them than it might pose to other adversaries.

Even if a theft of nuclear material did not result in a state or group gaining the ability to actually detonate a nuclear explosive, it might contribute substantially to the credibility of nuclear threats based on *claims* that they could do so. If enough material for a bomb was known to have been stolen from a particular site, for example, and a group sent in a threat to detonate a nuclear bomb if certain demands were not met, accompanied by a small sample of the stolen material, it would be difficult to dismiss the credibility of the threat. Such possibilities, while real, are not included in the consequence rankings in this chapter (or in the categorizations in U.S. or international regulations); if they were, they would have the effect of somewhat increasing the estimated consequences of small quantities of material (which still might be enough for a hoax, even if not for a bomb). If, on the other hand, stolen material never found a recipient who could make use of it (as appears to have been the case in the known cases of theft of HEU and plutonium to date), then the consequences of the theft could be quite minor.

Terrorist vs. State Recipients

The most important division among potential recipients is that between states and sub-state groups. As discussed in Chapter 2, states that had not yet succeeded in producing nuclear weapons or sufficient quantities of the materials needed to make them might be extremely interested in purchasing stolen weapons or materials. It is not hard to imagine thieves stealing nuclear material and selling it to a state, or a state-sponsored terrorist group stealing nuclear material and providing it to its state sponsor. A state would have far more financial, technical, human, and other resources than would a terrorist group and, with control of its own territory, would have a much easier time establishing a site where the work could be done without detection and disruption. Hence, a variety of barriers that might be significant for a terrorist group, such as the possible need to make an implosion-type rather than a gun-type bomb (and to carry out explosives tests with that objective), or the need to chemically process stolen material to recover the potential bomb material from it, would be much less significant for a state.[80] On the other hand, a state might be seeking not just a

[80] For a useful discussion of which barriers are more or less important in the case of "theft for a proliferation state" and "theft for a subnational group," see U.S. National Academy of Sciences, Panel to Review the Spent Fuel Standard for Disposition of Excess Weapons Plutonium, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options* (Washington, D.C.: National Academy Press, 2000; available at http://www.nap.edu/catalog/9999.html as of 15 August 2006), pp. 22-30.

crude, unreliable, unsafe bomb deliverable by a truck, but a usable military weapon with good safety and reliability, deliverable by missile or aircraft, which is a far more technically challenging goal to achieve.

Perhaps most important, the consequences if a terrorist group succeeded in getting a usable nuclear explosive capability from the stolen items would include a high probability of a nuclear detonation in a major city. By contrast, no state has actually used a nuclear bomb that it acquired since more than one state in the system possessed such weapons; even very hostile states are likely to be deterred from using a weapon in their possession against a city (particularly in a state with overwhelming military power, such as the United States) by the prospect of the overwhelming retaliation that would likely result if and when the source of the attack was identified.

Nevertheless, in the case of a state recipient, if the stolen material or nuclear weapon allowed that state to acquire a usable nuclear weapons capability that it otherwise could not have acquired (or could not have acquired as rapidly), this would be a substantial blow to U.S. and international efforts to stem the spread of nuclear weapons, posing a wide range of problems for U.S. foreign policy. It would increase the risk of nuclear use (by increasing the number of states that could make a decision to use nuclear weapons), and it would increase the risk of further nuclear proliferation, including to terrorist groups (by increasing the number of states that could serve as a source of a nuclear weapon or material, either by design or by inadvertence). It is extremely difficult to quantify these potential consequences, but two things are clear: (a) the consequences of additional states gaining nuclear weapon capabilities are substantial enough that the United States and many other countries have devoted enormous efforts to preventing this from occurring; but (b) these consequences are nevertheless dramatically smaller than those of the actual use of a nuclear weapon by a terrorist group.

Hence, despite the smaller probability of a terrorist recipient being able to get a usable ability to detonate a nuclear explosive from the stolen items, the overall consequences attributable to a terrorist recipient are likely to be substantially higher than those for a state recipient, except in those few cases where the stolen material would be so difficult to process into a bomb that the probability of success for a terrorist group seems very small. Even in those cases, however, security for the material in question cannot be entirely neglected, because of the possibility that the ultimate recipient will be a state, with a state's resources.[81]

To take a specific example of this difference between terrorist groups and states, consider the consequences of a theft of 1000 kilograms of low-enriched uranium (LEU), at a typical power reactor enrichment of 4.5% U-235. In this case, the probability that a terrorist

---

[81] In internal U.S. government discussions in the mid-1990s of what the criteria should be for terminating all domestic safeguards for certain nuclear materials, for example, advocates of criteria that would allow safeguards to be terminated on material that was up to 10% plutonium by weight, with no additional radiation barrier, argued that this was acceptable because terrorist groups would probably not be able to process such materials to make a bomb from them; even if that argument was correct (which in many of the cases in dispute I believe it was not), it neglected the possibility that the ultimate recipient would be a state. (Author's experience in interagency discussions of termination criteria, 1995-1997.)

group would be able to use it to make a nuclear bomb would likely be close to zero (because further enrichment would be required, which is almost certainly beyond the capabilities of terrorist groups).[82] A state recipient would only be able to use it to make a bomb if the state had an enrichment capability. But if that were the case, the state would have the capability to produce HEU for a weapon from natural uranium, even if it did not acquire stolen LEU. Having LEU available would reduce the enrichment work required to produce HEU dramatically, saving time and money, possibly making it possible to use lower-quality centrifuges (or other enrichment devices) and potentially making it easier to produce HEU covertly – but it would not be very likely to make acquisition of a nuclear weapon possible where it would otherwise be impossible.[83] Hence, the consequence in the case of a terrorist recipient would be very low, and the consequence in the case of a state recipient, while higher, would still be modest.

Categorizing Nuclear Materials: What Materials Should Get What Levels of Protection?

To efficiently allocate nuclear security resources to reduce the greatest risks, nuclear materials that recipients would have a larger chance of being able to make into a bomb should receive higher levels of protection, while nuclear materials that recipients would have only a low probability of making into a bomb should receive lower levels of protection. Both U.S. and international physical protection approaches are based on this principle of "graded safeguards." As the IAEA puts it, physical protection of nuclear material should be based on "the possibility that the unauthorized removal of plutonium, highly enriched uranium or uranium-233 could lead to the construction of a nuclear explosive device by a technically competent group," and protection levels should be based on a categorization of nuclear material into different classes "based on the potential risk of the material being used for a nuclear explosive device, which itself depends on: the type of material, e.g. plutonium, uranium; isotopic composition, i.e. content of fissile isotopes; physical and chemical form;

---

[82] For a discussion, see Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007), p. 18.

[83] One circumstance in which a state would find it very useful to have a secret source of LEU would be if the state were under full-scope International Atomic Energy Agency (IAEA) safeguards, but nonetheless attempting to operate a covert uranium enrichment plant to produce nuclear bomb material. In this case, starting from LEU rather than from natural uranium would mean that the needed enrichment plant to produce HEU for a bomb could be far smaller, and therefore somewhat easier to keep hidden. Starting with natural uranium (0.72% U-235), and leaving 0.3% U-235 in the depleted uranium or "tails," for example, an ideal enrichment cascade would require some 200 kilogram-separative work units (kg-SWU, often referred to simply as SWU) per kilogram of 90% HEU produced; if 4.4% enriched LEU was available, by contrast, and as much as 2% U-235 were left in the depleted uranium, only one-sixth as many SWU would be required per kilogram of HEU produced (and only 36 kilograms of LEU feed material would be needed per kilogram of HEU produced, compared to 220 kilograms of natural uranium feed for each kilogram of HEU). The author is grateful to John P. Holdren for providing an Excel file that implements the standard equations for making such calculations, which can be found, for example, in Allan S. Krass et al., *Uranium Enrichment and Nuclear Weapon Proliferation* (London: Taylor & Francis for the Stockholm International Peace Research Institute, 1983).

degree of dilution; radiation level; and quantity."[84] The ease or difficulty of making a nuclear bomb from a particular type of material is often described as its "attractiveness" to potential adversaries seeking a bomb, or its "utility" to them. The next sections of this chapter will focus on assessing the effect of each of these factors on the probability that recipients would be able to make a bomb from particular types of stolen material.

As nuclear security rules and procedures are set, the goal should be a balanced system of protection, in which, to the extent practicable, no particular type or quantity of nuclear material has such weak security measures that it poses a substantially greater overall risk of nuclear terrorism than any other. If one particular stockpile poses a particularly high risk, then resources should be applied to improve security for that stockpile until the risk there is no higher than elsewhere; but by the same token, if a particular stock already poses a low risk (because, for example, the amount of material there is too small to make a bomb), then resources should not be wasted on further improving security there when they could be spent improving security for other, higher-risk stockpiles. This implies, as will be discussed below, an approach that is more graded than current approaches are, so that the level of security required does not "fall off a cliff" when the material's characteristics pass some arbitrary regulatory threshold, beyond which it might still be quite useful in nuclear bombs.

In such a balanced approach to defining the levels of security required for different types and quantities of nuclear materials, policy-makers would:

(1) Define the level of risk of successful theft of the most attractive material (such as large quantities of HEU metal, or assembled weapons) that they are willing to accept, given the risks to society that might result from such a theft and the costs and difficulties of reducing the risk further;

(2) Set rules requiring sites with that type of material to provide security measures judged sufficient to reduce the probability of successful theft, given the expected spectrum of adversary capabilities, to the desired level;

(3) Estimate how much properties of nuclear material different from those of the most attractive material would reduce the probability that adversaries would be able to successfully make a nuclear bomb; and

(4) Set rules for these other types and quantities of nuclear material so that the *combined* risk of successful theft and successful bomb-making was no higher than the level of risk determined to be acceptable for the most attractive material.[85]

---

[84] International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities.*

[85] To fully optimize and ensure that all the most promising investments in improved security had been identified, one would also have to include the cost of achieving any given level of risk reduction. It may be, for one reason or another, that at particular sites large reductions in theft risks can be made for modest costs; in those cases, those investments should probably be made, even if those facilities are not among the highest-risk facilities overall. An analysis of the relative cost of all the reductions in theft risk that might be made at different nuclear facilities is far beyond the scope of this dissertation, however – and probably beyond the scope of the analysis governments can reasonably perform to support regulation and other nuclear security policies. At any *one* facility with weapons-usable nuclear material, however, procedures and software are available to assess the cost

More formally, the security system in such a balanced approach would be designed so that the overall risk of successful theft followed by successful bomb-making by potential adversaries was roughly constant over the different types of facilities and materials. For example, if policy-makers determined that sites with large quantities of HEU metal would have to demonstrate that their security measures would have a 95% chance of defeating theft attempts by the kinds of adversaries expected in that country – meaning only a 5% chance that such an attempt would be successful – and if they concluded that adversaries' chance of making a nuclear bomb from a particular different type of material would be only half as large (compared to their chance of making one from a large quantity of HEU metal), then if the security rules were set so that the security measures for the second type of material would not allow more than 10% of the theft attempts to be successful, the overall risk would be the same (assuming the probability of any type of theft attempt was constant among facilities with these different materials), with the probability of successful theft doubled but the probability of successful bomb-making cut in half.

In the discussion that follows, the reduction in the probability of successful bomb-making resulting from materials being less attractive than the best material is referred to as the "discount factor." This is normalized to 1.0 for nuclear weapons themselves and large quantities of HEU metal and is then somewhat lower for all other types of material. In the sections below, I provide very rough, preliminary estimates of such discount factors for a wide range of different types of nuclear material; I will then use these to propose a new approach to placing nuclear material into different categories requiring different levels of security measures, which would significantly modify current U.S. and international approaches.

Current Approaches to Categorizing Nuclear Materials

The approach to graded safeguards laid out in the IAEA's recommendations on physical protection and codified in the physical protection convention is based on three categories of nuclear material, with Category I material receiving the highest level of protection and Category III material the least. (Implicitly, there is a fourth category, the material not even included in the categorization scheme, which requires only "prudent management practices.") Table 4.3 shows how materials are categorized in this approach.

---

of a range of different approaches to achieving some required level of improvement in security (whether it be a larger design basis threat or a higher required probability of defeating that threat), and at some types of facilities (such as DOE facilities), such analyses of optimum upgrade approaches have become fairly routine. Such analyses of the relative costs and benefits of different improvements that could reduce risk are routinely made in the area of nuclear safety (usually by the companies operating the facilities); eventually, such analyses should become routine for nuclear security as well.

Table 4.3: IAEA Recommended Categorization of Nuclear Material

Material	Form	Category I	Category II	Category III[c]
1.Plutonium[a]	Unirradiated[b]	≥2 kg	<2 kg >500 g	≤500 g > 15 g
2.Uranium-235	Unirradiated[b]			
	Uranium enriched to ≥ 20% ^{235}U o	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15g
	Uranium enriched to 10% ^{235}U but less than 20%		10 kg or more	Less than 10kg but more than 1 kg 10 kg or more
	Uranium enriched above natural, but less than 10% ^{235}U			10 kg or more
3. Uranium-233	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated Fuel			Depleted or natural uranium, thorium or low-enriched fuel(less than 10% fissile content)[d,e]	

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 100 rad/hr at one meter unshielded.
[c] Quantities not falling in Category III and natural uranium should be protected at least in accordance with prudent management practice.
[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection. (INFCIRC/225 specifies that this level of protection is recommended for international transport considerations.)
[e] Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 100 rad/hr at one meter unshielded.

Source: International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Facilities,* INFCIRC/225 Rev. 4 (Corrected) (Vienna: IAEA, 1999, available as of 9 January 2007 at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html).

As can be seen, 2 kilograms or more of plutonium or U-233, or more than 5 kilograms of U-235 contained in HEU, are considered a Category I quantity of material. If the material is emitting 100 rad/hr at one meter or more, it can be reduced one category.[86] Plutonium isotopics do not affect the categorization, except that plutonium that is at least 80% by weight Pu-238 is excluded. Uranium isotopics above 20% do not affect the categorization. Spent fuel is included primarily because of international transport considerations – that is, fears of sabotage during the course of international transport. The chemical dilution and physical form of the material do not affect the categorization; plutonium-uranium mixed oxide (MOX) fuel, for example, would, in this approach, be protected in the same way that pure plutonium metal would be. In short, the approach is based primarily on the *quantity* of the material, with the *quality* of the material entering only in the 100 rad/hr threshold for "self-protecting" material, the 20% and 10% thresholds for different grades of enriched uranium, and the 80% Pu-238 threshold for excluding plutonium.[87]

The U.S. NRC regulations on categorizing material are similar in most respects (which is not surprising, since the IAEA recommendations were originally based in part on U.S. practices).[88] The limits on how much plutonium, U-235 in HEU, or U-233 constitute Category I, II, and III quantities in the NRC regulations are identical to those in the IAEA recommendations. The radiation level at which material is exempted from Category I security requirements is set at 100 rem/hr at three feet, essentially identical to the IAEA level.[89] The enrichment thresholds are the same, as is the lack of any distinction among materials with different chemical or physical forms. In recent rulings, however, the NRC has granted exemptions from many of its specific requirements for handling Category I material in the case of reactors that were planning to use fabricated MOX fuel, as discussed in more detail below.[90]

Since the late 1980s, DOE has taken a different approach, in which categorization is affected to a larger degree by the quality of the material under consideration. In addition to Categories I, II, III, and IV, the DOE system also includes attractiveness levels A, B, C, D,

---

[86] Because many of the physical protection rules in the United States and internationally were first established in the 1970s, before the SI units Grays and Sieverts came into common use, the regulations and discussions of them are still often framed in older units, and I will use these older units in this chapter. 1 Gray=100 rad; 1 Sievert=100 rem.

[87] The threshold of "less than 10% fissile content by weight" in reference to irradiated fuel is somewhat odd, as it does not specify how material that has 10% or more fissile content should be treated; from the rest of the table, a Category I quantity of such material, if it was emitting more than 100 rad/hr at one meter, would be treated as Category II, which is the same as the recommendation for spent fuel with lower fissile content. The purpose of this restriction to less than 10% fissile content by weight is therefore not clear.

[88] The NRC categorizations can be found in U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials."

[89] The U.S. rules are based on the roentgen-equivalent-man (rem) unit of absorbed dose. (1 Sievert=100 rem.) To convert from the radiation field to the absorbed dose requires multiplying by a "quality factor" that differs for different types of radiation; since, in the case of gamma rays, the quality factor is 1, in this case the 100 rem/hr at 3 feet standard and the IAEA-recommended 100 rad/hr at 1 meter standard are essentially equivalent.

[90] See, for example, U.S. Nuclear Regulatory Commission, *In the Matter of Duke Energy Corporation (Catawba Nuclear Station, Units 1 and 2)*, CLI-04-29 (Washington, D.C.: NRC, 2004; available at http://www.nrc.gov/reading-rm/doc-collections/commission/orders/2004/2004-29cli.pdf as of 22 September 2006).

and E, and if material is a chemical, physical, or isotopic form judged to be more difficult to make bombs from, it falls into a lower physical protection category. Table 4.4 outlines this DOE categorization approach.

As the table shows, the Category I quantities of "pure products" are the same in the DOE system as in the IAEA and NRC systems – although the DOE system includes separated americium and neptunium as well (discussed later in this chapter). But in the case of "high-grade materials," a larger quantity – just below the IAEA "significant quantity" figures for safeguards – is needed before the material qualifies as Category I. Materials classified as "low-grade" can never be Category I, even if tons of plutonium or HEU are present in them.

Several crucial particulars of the DOE system are not specified in Table 4.4, but are laid out in an old manual for implementing DOE's material control and accounting rules, which, at this writing, is in the process of being revised.[91] In particular, materials with any of the following characteristics are all considered "low-grade," and hence can never be Category I:

- Materials emitting at least 15 rem/hr at 1 meter (less than one-sixth of the IAEA self-protecting standard);
- Materials containing less than 10% by weight special nuclear material (that is, plutonium, U-235, U-233, americium, or neptunium), such as mixed oxide fuels containing 3-7% by weight plutonium and the rest U-238, for example;
- Uranium at enrichments below 50%.

In sufficient quantity, materials with any of these characteristics – and indeed, with all of them put together – would be treated as Category I in the IAEA system or the NRC system. This chapter will make the case that all three of these judgments on DOE's part are indefensible and should be revised. (As discussed below, however, the contrast may be less stark than it seems, as Category II material receives protection in the DOE system in many ways comparable to that recommended for Category I material by the IAEA.) Moreover, in the DOE system, material emitting 100 rem/hr or more at one meter is not just downgraded one category, it is considered "highly irradiated," and therefore downgraded all the way to Attractiveness Level E, which can never be more than Category IV material, requiring virtually no security measures to prevent theft (though DOE rules may specify important security measures related to sabotage, in some cases). Figure 4.2 provides a decision tree for DOE's categorization approach.

---

[91] U.S. Department of Energy, *Guide to Implementation of DOE 5633.3b, "Control and Accountability of Nuclear Materials"* (Washington, D.C.: DOE, 1995).

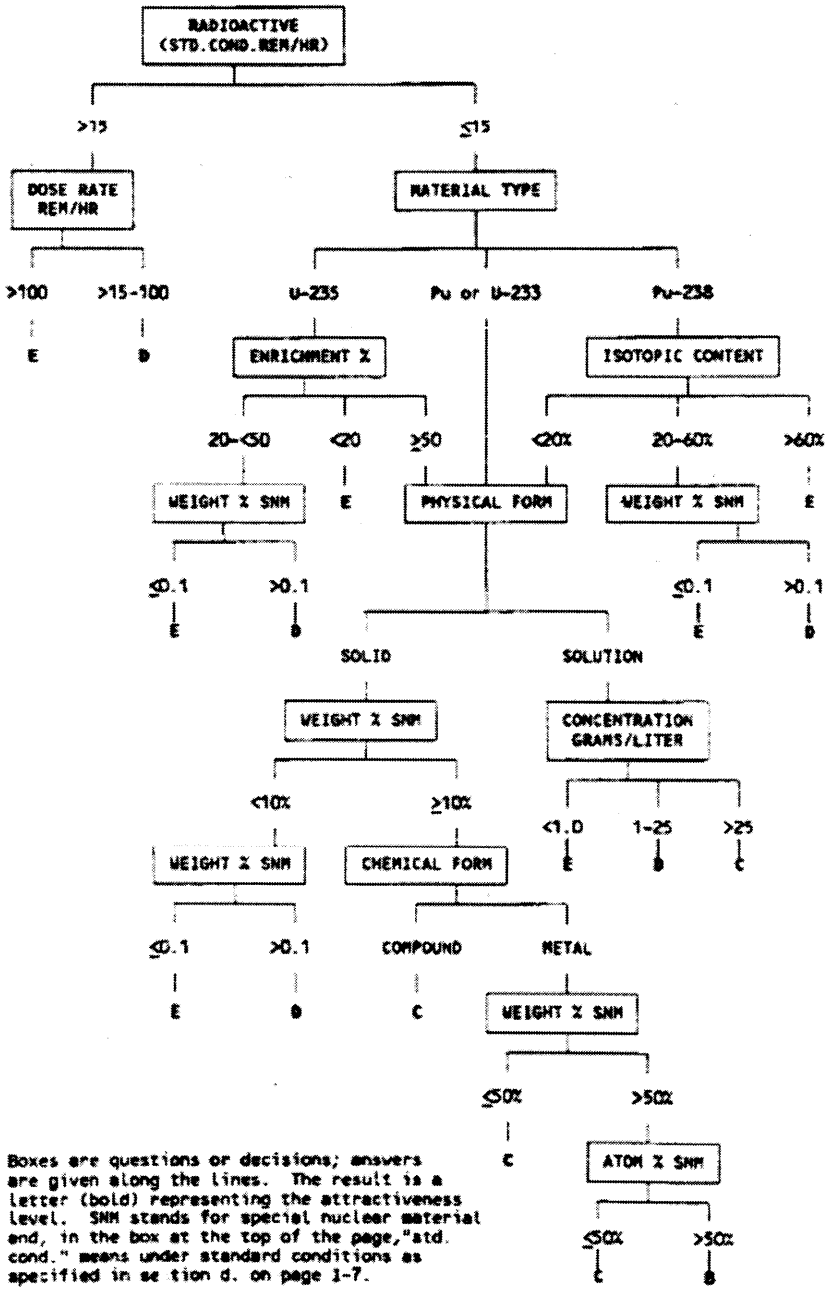
Table 4.4: DOE Table for Categorizing Nuclear Materials

	Attractiveness Level	Pu/U-233 Category (kg)				Contained U-235/Separated Np-237/Separated Am-241 and -243 Category (kg)				All E Materials Category IV
		I	II	III	IV[1]	I	II	III	IV[1]	
WEAPONS Assembled weapons and test devices	A	All	N/A	N/A	N/A	All	N/A	N/A	N/A	N/A
PURE PRODUCTS Pits, major components, button ingots, recastable metal, directly convertible materials	B	≥2	≥0.4<2	≥0.2<0.4	<0.2	≥5	≥1<5	≥0.4<1	<0.4	N/A
HIGH-GRADE MATERIALS Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF_4 or UF_6 (≥ 50% enriched)	C	≥6	≥2<6	≥0.4<2	<0.4	≥20	≥6<20	≥2<6	<2	N/A
LOW-GRADE MATERIALS Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); UF_4 or UF_6 (≥ 20% < 50% enriched)	D	N/A	≥16	≥3<16	<3	N/A	≥50	≥8<50	<8	N/A
ALL OTHER MATERIALS Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-233[2] (any form, any quantity)	E	N/A	N/A	N/A	Reportable Quantities	N/A	N/A	N/A	Reportable Quantities	Reportable Quantities

[1]The lower limit for Category IV is equal to reportable quantities in this Manual.
[2]The total quantity of U-233 = [Contained U-233 + Contained U-235]. The category is determined by using the Pu/U-233 side of this table.

Source: U.S. Department of Energy, *Nuclear Material Control and Accountability,* DOE M 470.4-6 (Washington, D.C.: DOE, 2005).

Figure 4.2: Decision-Tree for DOE Categorization System



Source: U.S. Department of Energy, *Guide to Implementation of DOE 5633.3b, "Control and Accountability of Nuclear Materials"* (Washington, D.C.: DOE, 1995).

Graded Safeguards, or Cliffed Safeguards?

The differences between the security measures recommended for Category I material and those recommended for all other material in the IAEA system are quite stark. This is important because, the way the rules are set today, some materials that might be quite useful in making a nuclear bomb are considered Category II or even less and are subject to very few security measures: these materials, under current circumstances, may pose substantial risks of nuclear theft and terrorism.

For Category I nuclear material, the IAEA recommends that it only be used in an "inner area" within a "protected area," with the ceiling, walls, and floor of the inner area designed to delay any attempt to penetrate them to remove material. The protected area should have a physical barrier around it with intrusion detection equipment and should have a 24-hour guard force in regular communication with offsite response forces; if the on-site guards are not armed, measures should be taken to compensate for that. Only people who have been cleared as trustworthy should be granted unescorted access to the protected area or the inner area. Everyone entering or leaving the inner area where the nuclear material is located should be searched. People in the inner area should be kept under "constant surveillance." When the material is being stored with no one present, it should be in a locked and alarmed "strong room" within the inner area.[92]

In the case of Category II material, by contrast, there is no need for an inner area; there is no need for a 24-hour guard force (though there should still be a central alarm station that is continuously manned); there is no need to keep the people in the material area under constant surveillance; and there is no need to store the material in a locked and alarmed strong room. On the other hand, the material should still be in a protected area with a physical barrier and intrusion detection around it, only cleared personnel should be given unescorted access to it, and all people, vehicles, and packages should be subject to search.[93] For Category III material, even these recommendations are eliminated.[94] While the IAEA recommendations call for all states to base their physical protection approaches on some specific DBT,[95] there is no requirement that this be applied to Category II and III material along with Category I material (even with less capable threats) – and as described below, the U.S. NRC, among others, only applies the DBT approach to Category I material. There are similarly stark differences in the recommendations for security for transport of these materials.

In general, the IAEA recommendations tend to be rule-based and say very little about how well the recommended security systems should perform. The recommendations call for each state to establish a design basis threat that nuclear security systems should be designed to defeat, but they do not make even general remarks about what levels of adversary capability

---

[92] See Section 6.2 in International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*.
[93] See Section 6.3 in International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*.
[94] See Section 6.4 in International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*.
[95] See Section 6.1 in International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*.

should be included. They call for a locked and alarmed strong room for storing Category I material, but there is no discussion of how strong the lock should be, how difficult to defeat the alarm should be, or how strong the strong room should be. They call for a 24-hour guard force for Category I material, but there is no discussion of how numerous or capable they should be (and as already noted, the guards do not necessarily have to have weapons to meet the recommendations, even if hundreds of kilograms of HEU metal are present). They call for an intrusion detection and assessment system, but there is no discussion of how effective and difficult to defeat this system should be – and so on.

The gap between the security required for Category I and Category II material is even greater in the NRC regulations.[96] Facilities with Category I material must have security arrangements capable of defeating a violent assault by a well-armed and well-trained group capable of operating in two or more teams or a conspiracy of well-placed insiders and they must have a substantial armed guard force.[97] The material must be in a material access area whose roof, walls, and floor each constitute a physical barrier (similar to the IAEA's inner areas) within a protected area. There are very detailed requirements for guard forces (including a Tactical Response Team of at least five armed guards to respond to any assault); physical barriers; intrusion detection, surveillance, and alarm systems; access controls; system testing; communications; and more.[98]

But facilities with only Category II material do not need to be protected against any particular DBT; they do not require an armed guard force; they do not have to be within a protected area with any kind of fence, or a material access area with any significant delay barriers.[99] In essence, Category II material has to be handled in an area to which access is controlled (in some unspecified way); when in storage, it has to be in some type of "vault-type room" or "security cabinet" (which may be a file cabinet with a padlock); there has to be some type of alarm in the case of unauthorized intrusion; and there has to be at least one watchman (who need not be armed and can have a variety of other duties as well). Material emitting 100 rem/hr at three feet is exempted even from these Category II requirements. All material that happens to be located at research reactors – even if it were large quantities of 90% enriched HEU – is exempt from all the Category I requirements, though there are very limited security requirements that are specific to research reactors with HEU emitting less than 100 rem/hr at three feet. In other words, HEU that would require a substantial armed guard force, fences, intrusion detectors, and a security plan able to defeat a specified DBT if it

---

[96] U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials."

[97] These requirements are in Sections 73.1, 73.46, and 73.50 in U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials."

[98] See Sections 73.46 and 73.50 in U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials."

[99] See Section 73.67 in U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials." It appears that the NRC regulations do not follow the IAEA recommendations, as the IAEA recommends that even Category II material be in a protected area with intrusion detection at the perimeter, but the NRC regulations do not require this. It is somewhat ironic that the United States has been inspecting other countries it supplies for thirty years to ensure that their physical protection arrangements are consistent with IAEA recommendations, when U.S. physical protection arrangements in some cases are not.

were located anywhere else does not require any of those things if it is located at a research reactor.[100]

In short, under NRC rules, a broad range of materials from HEU or plutonium metal to mixed compounds all require the same stringent level of protection; but if the quantity is small enough to put the material in the Category II category, or it is emitting 100 rem/hr at 1 meter or more, or it is at a research reactor, then the facility where the material exists is exempted from all of the most substantial security requirements. (Even the NRC requirements for Category I materials fall far below those at DOE: although the two major Category I facilities licensed by NRC (HEU processors Nuclear Fuel Services (NFS), in Erwin, Tennessee and BWXT Technology, in Lynchburg, Virginia) handle tons of HEU metal, the threats they are required to defend against are much less than those comparable DOE facilities must defend against.[101] That security levels should be determined by administrative status rather than risk assessment clearly does not make sense: from a societal risk perspective, either DOE is spending too much defending its HEU, or too little is being spent to protect the similar HEU at NFS and BWXT – whose work is largely paid for by DOE as well.)

At DOE, while a variety of materials are classed as Category II that probably should not be, the gap between Category I and Category II security appears not to be as large. (The most specific aspects of DOE security rules – and in particular its policy on what threats different types of facilities should be required to defend against – are not publicly available, so it is more difficult to base judgments on detailed reading of texts.) DOE's post-9/11 DBT for Category I material is very substantial – reportedly a highly trained, very well-armed force comparable in size to the 19 attackers who attacked on 9/11, along with potentially multiple insiders – and protecting DOE sites against this threat is proving to be very costly.[102]

---

[100] This exemption was intended to be temporary, as the research reactors phased over to LEU. For a discussion of some of the issues this poses, see Committee on Science, Space, and Technology, *Conversion of Research and Test Reactors to Low-Enriched Uranium (LEU) Fuel*, U.S. Congress, House of Representatives, 98th Congress, 2nd Session, 25 September 1984. More than two decades later, a substantial number of the NRC-regulated research reactors are still using HEU, and still have very little security in place. See, for example, "Radioactive Road Trip," "PrimeTime Live," *ABC News*, 13 October 2005.

[101] See, for exampleProject on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006).

[102] For discussions of the evolution of DOE's DBT over time since 9/11, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Y-12 and Oak Ridge National Laboratory at High Risk* (Washington, D.C.: POGO, 2006; available at http://pogo.org/p/homeland/ho-061001-Y12.html as of 17 November 2006). For an earlier discussion, with an explicit comparison to the less substantial DBT at NRC, see Project on Government Oversight, "Energy Ups Their DBT, NRC Still Making Excuses" (Washington, D.C.: POGO, 28 September 2004; available at http://pogoblog.typepad.com/pogo/2004/09/energy_ups_thei.html as of 5 December 2005). For a discussion of DOE's ongoing difficulties in meeting these new requirements, see Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *A Review of Security Initiatives at DOE Nuclear Facilities*, U.S. Congress, House of Representatives, 109th Congress, 1st Session, 18 March 2005 (available at http://energycommerce.house.gov/108/Hearings/03182005hearing1457/hearing.htm as of 15 August 2005).

(Spending on all safeguards and security at DOE is now in the range of $1.5 billion per year.[103])

At DOE facilities, Category I material must be located in a material access area with specific types of physical barriers, entry and exit inspections, and access controls, to which armed guards can respond more rapidly than adversaries could complete their task – either setting off a bomb on-site or stealing material – after setting off an alarm.[104] Such material access areas have to be located within protected areas, each of which must have a perimeter intrusion detection and assessment system (PIDAS) which has been tested to assure that it will detect intruders at least 90% of the time.[105] Category II material must also be within a protected area with such a PIDAS, but it need not be in a material access area.[106] Category II material must be protected against a DBT that is "significantly less" than the Category I threat[107] – but Category II material still has to be protected against *some* specified threat, unlike the NRC approach. In the DOE system, material emitting more than 100 rem/hr at one meter, classified as Category IV, requires very little security against theft (though in some cases some security measures may be employed to protect against sabotage).

Overall, in these systems, except perhaps for the DOE system, "graded safeguards" might be more accurately described as "cliffed safeguards." While the risks particular types of material pose do not change substantially as the amount of plutonium increases from 1.9 kilograms to 2.1 kilograms, or the radiation level it emits decreases from 101 rem/hr at one meter to 99 rem/hr at one meter, the difference in the required levels of security is dramatic. If the objective is to allocate protection resources efficiently to reduce the overall level of risk from all materials that could be used in nuclear weapons, then a more graded approach is needed that does not have such dramatic security "cliffs".

These categorization systems have had major consequences, leaving some high-risk nuclear material around the world almost unprotected. U.S. teams cooperating with Russia to improve security for nuclear materials, for example, have been instructed to focus almost exclusively on material that would be considered "high-grade material" or "pure products" in DOE's categorizations, leaving large quantities of only lightly irradiated HEU, or fuel elements with less than 10% by weight plutonium or HEU, without improved security.[108] The Material Conversion and Consolidation (MCC) program that has worked with Russia to remove HEU from vulnerable civilian sites and blend it down to LEU, operating under similar guidelines, has in most cases focused on "high-grade material" or "pure products" –

---

[103] U.S. Department of Energy, *FY 2007 Congressional Budget Request: Other Defense Activities*, vol. 2, DOE/CF-003 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_2_ODA.pdf as of 22 December 2006), p. 161.

[104] See Section IV.8 in U.S. Department of Energy, *Physical Protection*, DOE M 470.4-2 Chg. 1 (Washington, D.C.: DOE, 2006).

[105] See Section VII.3 in U.S. Department of Energy, *Physical Protection.*

[106] See Section II.8 in U.S. Department of Energy, *Physical Protection.*

[107] Personal communication from Amy Whitworth, National Nuclear Security Administration, Office of Field Security, June 2006.

[108] This instruction is incorporated in the official guidelines for the program; these are not publicly available, however.

categories that do not include a large fraction of the HEU research reactor fuel in Russia.[109] The U.S. effort to ensure that U.S.-supplied HEU at research reactors around the world was adequately secured did not review or improve security for irradiated HEU fuel at all until recently – assuming, incorrectly, that this material met the "self-protecting" standard and therefore that it required little security.[110] Research reactors in a number of countries attempt to manage their fuel loading and unloading to keep their irradiated HEU fuel above the 100 rad/hr at 1 meter limit, so as not to have to implement more substantial security measures.[111]

The next sections of this chapter are focused on assessing how changes in the quantity and quality of material affect the probability of successful bomb-making – information that can then be used in assessing how much protection these different materials should be afforded. This will make it possible to make judgments about the validity of existing rules and to offer an alternative approach to categorizing what nuclear materials require what levels of protection.

Different Materials and the Spectrum of Recipient Capabilities

Whether considering terrorist groups or states as potential recipients, the key question is how *much* lower is the probability that a potential recipient using materials other than the reference large quantities of HEU metal would succeed in making a nuclear bomb from them?

For the question to even come up in the case of a terrorist group recipient, a terrorist group would have to be (a) sophisticated enough to be able to organize a successful effort to acquire some form of weapons-usable nuclear material (either by stealing it itself, getting it from others who had done so (possibly through intermediaries on some sort of black market), or acquiring it from a state); and (b) technically capable enough to be able to make at least a crude nuclear explosive if it got a large quantity of HEU metal. Hence, we are, in effect, zooming in on one part of the spectrum of possible adversary capabilities and asking: among the small subset of groups with the sophistication likely to be needed to acquire nuclear material and capable of making at least a crude bomb if they got the most attractive nuclear material, what portion would *also* have the sophistication to overcome whatever additional barriers are created by the less attractive nuclear material under discussion – and how might the odds of them making a project-ending mistake be changed by these additional barriers?

To make this approach concrete, consider what discount factor should be applied to a potential theft of 20 kilograms of 80% enriched HEU in the form of lightly irradiated

---

[109] This is apparently not an absolute constraint, however; on some occasions, the program has accepted limited amounts of material in lower DOE attractiveness categories, if some particular goal (such as clearing all the HEU out of an entire building) would be achieved by doing so. Personal communication from DOE official, October 2006.

[110] See Philip Robinson, "Global Research Reactor Security Program," in *RERTR 2005: 27th International Meeting on Reduced Enrichment for Research and Test Reactors, Boston, Mass., 6-10 November* (Argonne, Ill.: Argonne National Laboratory, 2005).

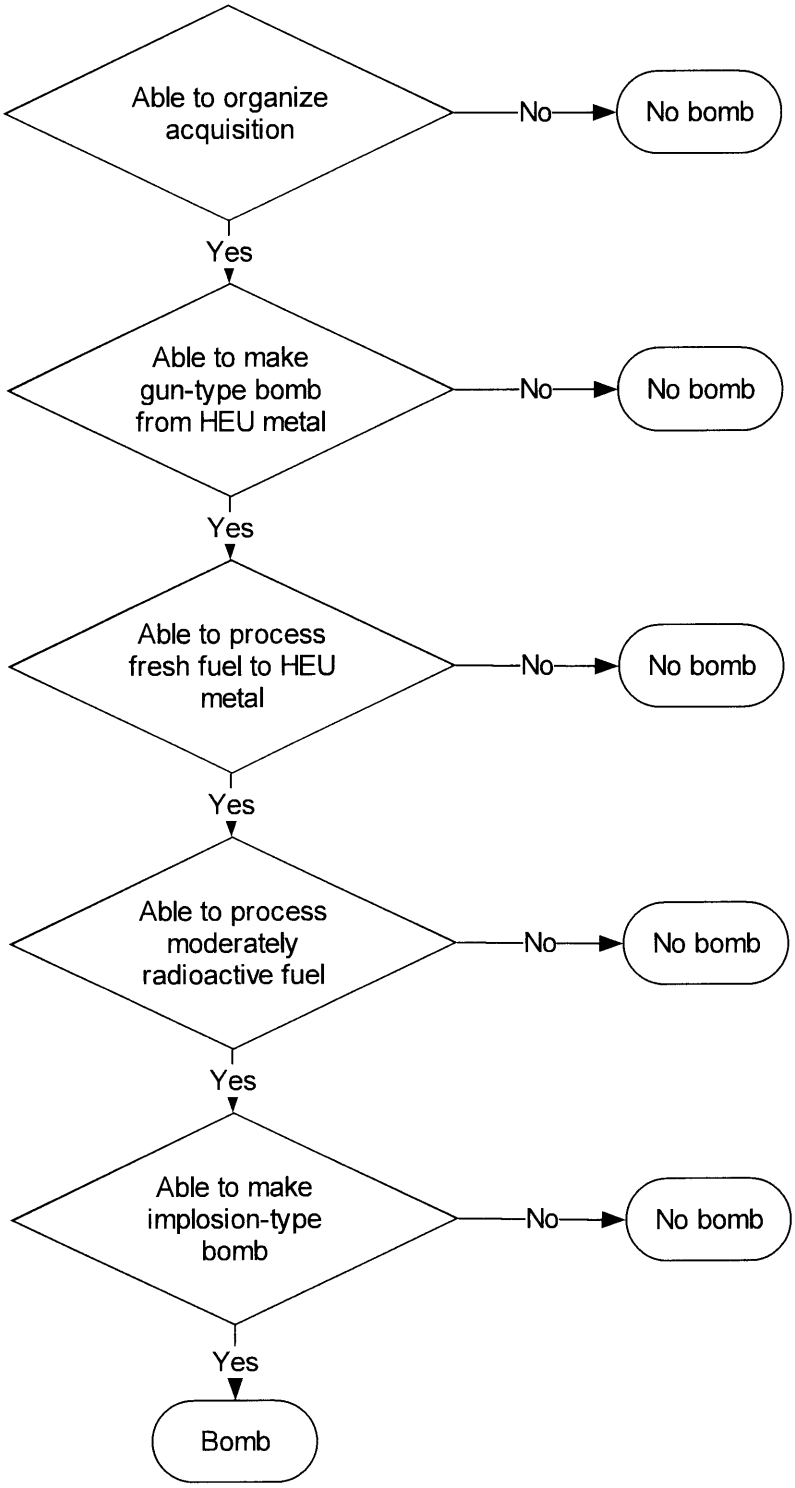
[111] For a discussion of the difficulties of operating reactors to maintain more than 100 rad/hr at 1 meter at all times, see J.J. Koelling and E.W. Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II*, vol. LA-9213-MS, NUREG/CR-2492 (Washington, D.C.: U.S. Nuclear Regulatory Commission, 1982; available at http://www.sciencemadness.org/lanl1_a/lib-www/la-pubs/00307470.pdf as of 28 September 2005).

uranium-aluminum oxide research reactor fuel (a very common type of material managed with very modest security in facilities all over the world). As discussed below, this amount of material would probably not be sufficient for a simple gun-type bomb; a more complex implosion bomb would likely be required. Moreover, the research reactor fuel would have to be chemically processed to separate the uranium from the aluminum – in the presence of at least a modest level of radiation – and then the recovered uranium would have to be processed to metal. For theft of this material to result in a usable nuclear explosive in the hands of a terrorist group, the adversary recipient would have to (a) be sophisticated enough to organize the needed effort to acquire the material; (b) in addition, be technically capable enough to take a large quantity of HEU metal and make a gun-type bomb from it; (c) in addition to that, be capable of making a more difficult implosion-type bomb; (d) in addition to that, be capable of chemically processing the research reactor fuel to get HEU metal from the uranium-aluminum oxide; and (e) in addition to that, be capable of doing the chemical processing in the presence of at least a modest level of radiation. If it lacked any of these capabilities, no bomb would result. See Figure 4.3.

If the probability of a terrorist group having each of these capabilities were entirely independent, then the total probability of succeeding through such a long chain would in most cases be quite small, even if the probabilities at each step were substantial. Unfortunately, however, these probabilities are likely to be closely linked. A terrorist group with the size, sophistication, and nuclear ambitions that would be required to acquire nuclear material and be able to make a bomb from a large amount of HEU metal would very likely be sophisticated enough to determine what additional technical capabilities it needed for other weapons-usable material, which of these capabilities it could get and then proceed to acquire them.[112] On the other hand, the probabilities of making a project-ending mistake at any particular step are likely to be more nearly independent, and the probability of the conspiracy being detected and stopped is likely to grow as the needed effort becomes more complex and time-consuming. Hence, the chance that a terrorist group that could get and make a bomb from enough HEU metal for a gun-type bomb would also succeed in making a bomb from enough irradiated research-reactor HEU for an implosion-type bomb is substantially less than 100% – perhaps in the range of 20-50% – but it is not likely to be in the range of 0-5%.

[112] Hence, the argument that the probability of nuclear terrorism is low because there are only a small proportion of terrorist groups willing to attack the United States; a small proportion willing to kill people indiscriminately; a small proportion willing to use nuclear weapons; and a small proportion capable of doing so, so that the proportion that is simultaneously in all of these categories is vanishingly small, is not correct. These characteristics of terrorist groups are almost certainly very strongly correlated, rather than independent; one would guess, for example, that there is almost 100% overlap between groups willing to kill indiscriminately and groups willing to use nuclear weapons. (This argument, with an accompanying Venn diagram, is attributed to David Tucker, in Corine Hegland and Gregg Webb, "The Threat," *National Journal* 37, no. 16 (15 April 2005; available at http://nationaljournal.com/about/njweekly/stories/2005/0415nj1.htm as of 30 December 2006).

Figure 4.3: Capabilities Needed to Make a Bomb from 20 kg of HEU in Irradiated Research Reactor Fuel



Different terrorist groups will vary in their ability to overcome the various barriers posed by different types of material without being detected or making fatal mistakes. Figure 4.4 provides a notional representation of the probabilistic spectrum of plausible recipient capabilities. As with Figure 4.1, it is intended only to be illustrative, not definitive – in some cases, a plausible case could be made for moving a particular capability one step up or down on this graph, or for arguing that a particular capability is so difficult that there should be a large probability gap between one capability and the next. A large gap is shown, for example, between the ability to process nuclear material that is not radioactive enough to require remote handling and the ability to do complex chemical processing remotely, or to enrich uranium. (Most analysts believe that the likelihood of a terrorist group being able to enrich uranium on its own is extremely small.) Later in this chapter, each of these types of barriers posed by the quantity and quality of the materials that might be stolen will be discussed in much more detail. This chart refers to recipients that are sub-national groups; a similar chart for state recipients would likely have most of the early points in Figure 4.4 clustered in the high probability region, as these are tasks that most states would likely be able to carry out, with sufficient determination.

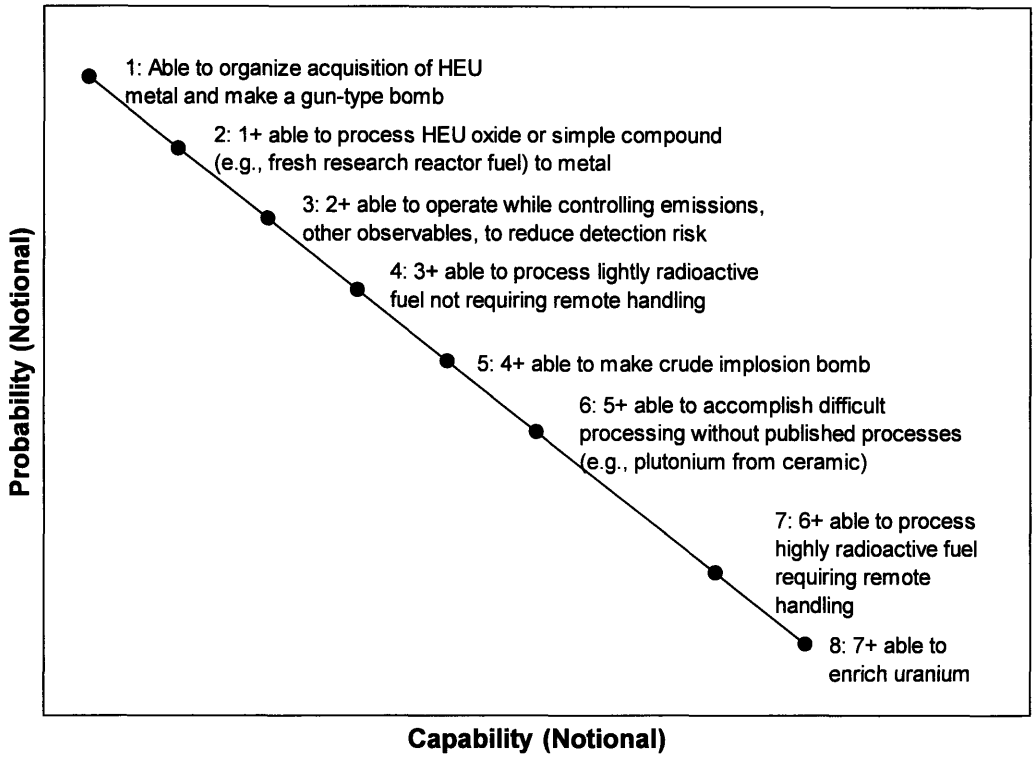
In assessing the probability that thieves might bring to bear various capabilities, numerous somewhat analogous cases are available to draw on, provided by past thefts of valuable guarded items and past terrorist attacks. A similar record of analogous cases of terrorist or criminal capabilities in chemical processing of nuclear materials, plutonium and uranium metallurgy, and nuclear physics is not available (fortunately). On the one hand, as discussed in Chapter 2, the nuclear weapons effort of even the Japanese terror cult Aum Shinrikyo – an unusually large and well-financed terrorist group with many technically trained members – was almost comically inept and did not proceed very far. And from what little is known about al Qaeda's nuclear efforts, it too seems to have made only modest progress – though the possibility that cells linked to al Qaeda have secretly made much more progress than is known cannot be ruled out.

On the other hand, terrorists and criminals have repeatedly demonstrated considerable sophistication in the use of explosives of various types and, in some cases, in chemical processing – particularly in the manufacture of illegal drugs. In the case of manufacturing heroin, for example, some steps involve handling material that is quite toxic if inhaled, and glove-boxes not dissimilar from those used in the nuclear industry are often used.[113] The widespread manufacture of drugs from methamphetamine to LSD demonstrates the crude but effective chemical processing that even relatively small subnational groups have been capable of when the incentive was right. Overall, however, judgments related to what kinds of capabilities in machining, chemical processing, and the like adversaries might have, with what probability, have to be based primarily on technical judgment, given the modest past experience with such adversary operations.

---

[113] As far as I am aware, this analogy was first raised by Theodore B. Taylor in Robert B. Leachman and Phillip Althoff, *Preventing Nuclear Theft: Guidelines for Industry and Government* (New York: Praeger, 1972), p. 283.

Figure 4.4: The Probabilistic Spectrum of Capabilities of Plausible Recipients



The Difference Between Gun-Type and Implosion-Type Bombs

One of the most important distinctions among different types of nuclear material is whether the material can be used to make a simple "gun-type" nuclear bomb, or whether it can only be used for a much more challenging "implosion-type" bomb.

The basic problem in making a fission bomb is getting enough nuclear material together fast enough so that the reaction does not start going and blow the material apart before it can generate an appreciable explosive yield. More specifically, to get a significant nuclear explosive yield requires getting a mass of nuclear material together that is supercritical on prompt fast neutrons,[114] and keeping it that way for enough fission

[114] A mass arranged in such a way that the neutrons from one fission, on average, lead to the fission of more than one other atom (in the next "generation" of fission), so that the rate of the reaction grows exponentially, is referred to as "supercritical." Nearly all of the neutrons released when atoms fission are released immediately – the "prompt" neutrons – but a few are delayed. A nuclear power plant is designed to be just critical, so that the pace of the nuclear reaction is neither increasing nor decreasing, with both the prompt and the delayed neutrons; by contrast, a nuclear bomb must be supercritical, with the pace of the reaction growing exponentially, on prompt neutrons alone. Moreover, most nuclear reactors slow the neutrons released in fission down (using what is known as a neutron "moderator," typically water or graphite), taking advantage of the fact that slow (or "thermal") neutrons have a far better chance of splitting an atom of U-235 or Pu-239 than fast neutrons do; nuclear bombs cannot take the same approach because the neutrons would then be traveling too slowly to fission

generations to split some noticeable fraction of the atoms in the nuclear material. The fundamental problem is that the nuclear chain reaction is likely to begin as soon as the material is critical and a neutron splits an atom, releasing more neutrons; as the chain reaction occurs, the energy it releases will quickly heat up the nuclear material, turn it to vapor, and cause it to expand to a point where the material is no longer critical, thus stopping the chain reaction. The trick is to get a substantial amount of material fissioned before this occurs, given the presence of background neutrons.[115]

As described in Chapter 2, two principal means of accomplishing this have been developed, though there are many variations: a gun-type bomb, in which two (or more) subcritical pieces of nuclear material are slammed together at high speed, or an implosion-type bomb, in which explosives surrounding a subcritical mass of nuclear material compress it until it becomes supercritical and an explosive chain reaction begins.

In dealing with the problem of background neutrons and pre-initiation, the key difference between the two types of designs is the characteristic assembly time. In a typical gun-type bomb slamming two pieces of HEU together, the assembly might become critical when the two pieces are still some 20 centimeters apart; if they are traveling at a relative velocity of 300 m/sec, it will take them just under a millisecond to travel this distance and reach maximum supercriticality; if the reaction begins before they have finished traveling this distance, the yield will be dramatically reduced.[116] In an implosion-type bomb, by contrast, the material is moving a few centimeters at a velocity just over half the shock velocity of the explosives, which might be in the range of 7-8,000 m/sec, so the assembly time is more of the order of tens of microseconds. Hence, a high-yield gun-type bomb can readily be made using 90% enriched HEU, with its low neutron background – but any attempt to make a gun-type bomb from plutonium would produce only a tiny nuclear yield.[117] Weapon-grade plutonium,

---

much of the material before it expanded and the reaction stopped. See, for example, discussion in Robert Serber, *The Los Alamos Primer: The First Lectures on How to Build an Atomic Bomb* (Berkeley: University of California Press, 1992), pp. 9-20.

[115] For the best available unclassified discussion of the basic physics problem to be solved in making a nuclear bomb, see Serber, *The Los Alamos Primer*.

[116] Serber, *The Los Alamos Primer*, pp. 45-61. For a discussion using the same typical numbers of a 20 cm distance and a 300 m/sec speed, see Alexander Glaser, "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Levels," *Science and Global Security* 14 (2006).

[117] A kilogram of U-235 undergoes 5.60×10^{-3} spontaneous fissions per second, generating .010 neutrons/sec, while a kilogram of U-238 undergoes 6.78 spontaneous fissions per second (over 1200 times the rate for U-235), generating 13.6 neutrons per second. (For a useful discussion of these rates and their implications, see Glaser, "Proliferation Potential of Uranium Fuel." Glaser's figures on spontaneous fissions are consistent with those that can be derived from the data provided in "Chart of Nuclides" (Upton, N.Y.: Brookhaven National Laboratory, 2006; available at http://www.nndc.bnl.gov/chart/ as of 9 January 2007).) Hence a bare-sphere critical mass of 50 kilograms of 93% enriched uranium, suitable for making a gun-type bomb, would generate just under 50 neutrons per second if it contained no other impurities. As will be discussed later in the text, α-n reactions with light-element impurities might contribute roughly another 25 neutrons per second in such a 50 kilogram sphere. With the material emitting some 75 neutrons per second, on average, it is reasonably straightforward to get the pieces of a gun-type bomb together rapidly enough to achieve a low probability of predetonation. By comparison, a kilogram of Pu-239 undergoes 7.11 spontaneous fissions per second, and a kilogram of Pu-240 undergoes 478,000 spontaneous fissions per second. Hence, a kilogram of typical weapon-grade plutonium containing some 94% Pu-239 and roughly 6% Pu-240 would undergo some 29,000

however, can be used in an implosion-type design with only a modest risk of pre-initiation leading to a much reduced yield.[118]

A gun-type bomb is also very inefficient, however, requiring far more nuclear material than needed for an implosion-type bomb. The Hiroshima bomb, for example, which was a gun-type weapon, used approximately 60 kilograms of HEU metal, with an average enrichment of 80%.[119] If the nuclear material the recipients got was plutonium, or a quantity of HEU too small for a gun-type bomb, they would have to build a more complex implosion-type bomb to get a substantial nuclear explosive yield.

Published sources report a broad range of views as to how much more difficult it is to design and build an implosion bomb, compared to a gun-type bomb. At one end of the spectrum, Luis W. Alvarez, a Nobel laureate in physics and a participant in the Manhattan Project, argued that getting a substantial nuclear yield from enough weapon-grade HEU for a gun-type bomb was a "trivial job" which "a high school kid" could do "in short order," whereas making an implosion-type bomb "is the most difficult technical job I know."[120] At the other end of the spectrum, a 1977 report from the Office of Technology Assessment argued that the difficulties of designing and building a gun-type device or an implosion-type device are "roughly equivalent."[121]

After consulting with a number of nuclear weapon designers, I conclude that the truth lies in between these extremes. A crude terrorist gun-type device that would not require high reliability, safety, or efficiency would be substantially simpler to construct than an implosion-type device – but is not likely to be something a single high-school kid could accomplish. In most cases, even making a gun-type bomb from HEU metal will require a team that includes someone who understands at least the basics of the nuclear physics involved in a nuclear

---

spontaneous fissions per second, and a roughly 10-kilogram bare-sphere critical mass of such material would undergo some 290,000 spontaneous fissions/second, generating roughly twice that number of neutrons/second. (This ignores the contributions from other minor isotopes, but these are small in weapon-grade plutonium; the result given here is quite similar to that for more complete calculations based on the composition of typical weapon-grade plutonium, ranging from 52,000 to 66,000 neutrons/kg-sec (see U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 45; J. Carson Mark, "Explosive Properties of Reactor-Grade Plutonium," *Science and Global Security* 4 (1993; available at http://www.princeton.edu/%7Eglobsec/publications/pdf/4_1Mark.pdf as of 9 January 2007). The distance the assembly has to travel from first criticality to the moment of optimum criticality decreases with the cube root of the mass (see Glaser, "Proliferation Potential of Uranium Fuel," p. 22.) With weapon-grade plutonium having one-fifth the critical mass of 90% enriched HEU, the distance to be traveled while critical would be cut almost in half, but with the huge neutron rate, one would still expect over 200 neutrons during the period before optimum criticality. In the case of reactor-grade plutonium, with its higher content of Pu-240, the neutron generation is roughly six times worse. See U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 45; Mark, "Explosive Properties of Reactor-Grade Plutonium."

[118] For discussion, see Mark, "Explosive Properties of Reactor-Grade Plutonium."

[119] Serber, *The Los Alamos Primer*, pp. xv, 22.

[120] Luis Alvarez, *Adventures of a Physicist* (New York: Basic Books, 1987), p. 125.

[121] U.S. Congress, Office of Technology Assessment, *Nuclear Proliferation and Safeguards* (Washington, D.C.: OTA, 1977; available at http://www.wws.princeton.edu/ota/disk3/1977/7705/7705.PDF as of 12 December 2006), p. 142.

explosive; some one able to melt uranium metal and cast it into appropriate shapes for the two HEU pieces the gun should slam together; some one able to machine the cast pieces of uranium metal (a metal with somewhat unusual properties) to at least reasonably precise specifications; some one familiar enough with explosives and gun ballistics to be able to arrange a gun to fire the HEU pieces together appropriately; and some care to ensure that neither noises nor effluents from the group's work could be easily detected.[122] A crude implosion-type device would pose a substantially greater challenge for a subnational group, but would not require as extreme a level of sophistication as is sometimes imagined. In particular, as long as a substantial degree of compression is achieved, the imploding shock wave does not have to be perfectly shaped. (A flat platter charge placed against a flat plate of steel will result in substantial compression of the steel.) There is a very real possibility that a technically sophisticated terrorist group, given sufficient effort, could make a crude implosion-type bomb – particularly if they succeeded in recruiting knowledgeable help, as al Qaeda in particular has been actively attempting to do.

There would, however, be a number of difficulties that would be greater on the implosion path. The group would have to not only design but manufacture a set of explosives that could be detonated with reasonably precise timing and that would be able to crush a ball of material into a denser configuration. For a group without previous experience, estimating how much compression was likely to be achieved in their design would be a very difficult problem, almost certainly requiring a number of explosive tests to clarify; depending on the location where this testing was conducted, this might increase the danger of detection. Moreover, instrumenting such tests to assess how well the explosives are working in compressing the ball of metal is itself a tricky problem; flash X-rays were used for this purpose in the early days of the Manhattan Project, and flash X-ray technology is controlled by the Nuclear Suppliers Group.[123]

A variety of official U.S. government studies, from the 1970s through to the present, have similarly concluded that terrorist groups might well be able to make crude nuclear bombs of either the gun-type or the implosion-type.[124] The U.S. Department of Defense has offered a view very similar to that taken in this chapter:[125]

---

[122] For a discussion of these requirements, see, for example, J. Carson Mark et al., "Can Terrorists Build Nuclear Weapons?" in *Preventing Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Lexington, Mass: Lexington Books, 1987; available at http://www.nci.org/k-m/makeab.htm as of 4 January 2006).

[123] I am grateful to Michael Levi for making this point. Personal communication, June 2006.

[124] For a discussion from the 1970s, see U.S. Congress, *Nuclear Proliferation and Safeguards*. For official U.S. government discussions from the late 1990s, see, for example, U.S. Department of Energy, Office of Arms Control and Nonproliferation, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*, DOE/NN-0007 (Washington, D.C.: DOE, 1997; available at http://www.osti.gov/bridge/servlets/purl/425259-CXr7Qn/webviewable/425259.pdf as of 2 January 2007); U.S. Department of Defense, "Section V: Nuclear Weapons Technology," in *Militarily Critical Technologies List* (Washington, D.C.: DOD, 1998; available at http://www.fas.org/irp/threat/mctl98-2/p2sec05.pdf as of 12 December 2005). In the discussion of the barriers posed by different types of materials that follows, I will be referring frequently to this DOE report and to other reports from committees of the National Academy of Sciences, from a DOE-sponsored group known as the Proliferation Vulnerability Red Team, and from another laboratory group led by experts at the Lawrence Livermore National Laboratory. In the

> If fissile material is available, subnational or terrorist groups can likely produce an "improvised nuclear explosive device" which will detonate with a significant nuclear yield...A terrorist with access to >50 kg of HEU would almost certainly opt for a gun-assembled weapon despite the inherent inefficiencies of such a device, both because of its simplicity and the perceived lack of a need to test a gun assembly... If the subnational group had only ^{239}Pu or needed to be economical with a limited supply of HEU, then it would likely turn to an implosion assembly.

Similarly, a 1987 article on the plausibility of terrorists making nuclear weapons by several key nuclear weapons scientists from Los Alamos, including experts in physics, metallurgy, and explosives – probably the most detailed authoritative statement on the subject in the unclassified literature – makes only modest distinctions between the difficulties of gun-type and implosion-type weapons.[126]

How *much* lower is the probability that a terrorist group could make an implosion-type bomb than the probability that they could make a gun-type bomb? There are probably a substantial number of terrorist groups that could plausibly get some significant nuclear yield if presented with a large quantity of weapon-grade HEU metal, but that would *not* be likely to be able to get a noticeable nuclear yield from plutonium. But if one focuses in, as one should, on the small subset of groups with the sophistication needed both to organize a successful acquisition of nuclear bomb material *and* to make a gun-type bomb, it seems very likely that the majority of them would also have the capability – or be able to acquire the capability – to make a crude implosion-type bomb. At the same time, the probability of being detected and stopped, or of making a mistake that would lead to an unworkable bomb, would certainly be higher for an implosion bomb. (Most states would likely be able to make either a gun-type or

---

interest of full disclosure, I should note that I was the principal drafter of this DOE report, and was the study director for the 1994 and 1995 Academy studies. U.S. National Academy of Sciences, Committee on International Security and Arms Control, *Management and Disposition of Excess Weapons Plutonium* (Washington, D.C.: National Academy Press, 1994; available at http://books.nap.edu/html/plutonium/0309050421.pdf as of 30 December 2006); U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*. Hence, while these studies represent official U.S. government or Academy publications, they are not entirely independent of my own thinking. By contrast, I had no substantial role in the 2000 Academy study of the spent fuel standard, in the Proliferation Vulnerability Red Team, or in the Livermore-led laboratory group (though the latter reported to an advisory committee of which I was a member). See U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*; Hinton et al., *Proliferation Vulnerability Red Team Report*; "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," in *Technological Opportunities to Increase the Proliferation Resistance of Global Nuclear Power Systems (TOPS)* (Washington, D.C.: U.S. Department of Energy, Nuclear Energy Research Advisory Committee, 2000; available at http://www.nuclear.gov/nerac/FinalTOPSRptAnnex.pdf as of 9 January 2007).

[125] U.S. Department of Defense, "Nuclear Weapons Technology." The first sentence quoted is a summary conclusion from p. II-V-58 ; the others are from the section "Types of Nuclear Design Useful for a Terrorist" on pp. II-V-60-61. On p. II-V-60, the document also remarks that "90 percent of the overall difficulty in making a nuclear weapon lies in the production of special nuclear material," noting that more than 90 percent of the Manhattan Project budget went to material production, with only 4 percent to the scientific laboratory at Los Alamos.

[126] Mark et al., "Can Terrorists Build Nuclear Weapons?"

an implosion-type bomb, given enough time, if they were the recipients.) Overall, I estimate that the probability that the high-capability terrorist groups under consideration here would succeed in making an implosion-type bomb is in the range of 40-60% of the probability that they would succeed in making a gun-type bomb. For the purposes of this chapter, if a large quantity of HEU metal has a discount factor of 1.0, I will assign a discount factor of 0.6 to plutonium metal or a quantity of HEU metal insufficient for a gun-type bomb.[127]

In short, the argument here is that while large quantities of HEU metal pose the highest risks, the risks posed by plutonium are substantial and cannot be ignored. This represents, in a sense, a balance between authors who would assign a much lower probability to terrorists being able to make an implosion-type bomb and official practices that make no distinction between plutonium and HEU. In the DOE system, for example, while considerable effort has gone into analyzing the consequences of theft of different types of material, theft of HEU or of plutonium are considered to have equal consequences. Similarly, in international recommendations for securing nuclear material, substantial quantities of either HEU or plutonium are considered to require equal levels of security.

Material Quantity and Theft Risk

The frequent question "how much HEU or plutonium does it take to make a bomb?" has no one technical answer – it depends on the sophistication of the bomb-maker. To get a substantial yield from a gun-type device typically requires something of the order of one bare-sphere critical mass of HEU (some 50 kilograms, in the case of 93% enriched weapon-grade uranium). Criticality can be achieved with half of a bare-sphere critical mass or less with the use of an appropriate neutron reflector, but since reasonable efficiency in a gun-type device requires the presence of something like two critical masses,[128] a single bare-sphere critical mass is a reasonable figure for a gun-type bomb. For example, as noted above, the Hiroshima bomb used some 60 kilograms of material with an average enrichment of 80%. A gun-type weapon can be made using smaller quantities of material than one bare-sphere critical mass, but the yield declines very sharply as the quantity of material is reduced.[129]

Implosion-type weapons, which compress the nuclear material to a higher density, are more efficient and require less nuclear material. In the case in which the implosion crushes

---

[127] Another aspect of the consequences of nuclear theft, in the case of plutonium, is that even if a group failed to manufacture a bomb that produced a substantial nuclear yield from plutonium, the result could be a radiological dirty bomb contaminating a substantial urban area. (Uranium is not very radioactive and would not be especially useful for use in a dirty bomb.) For a useful discussion of the consequences of dispersal of a bomb's worth of plutonium, see, for example, Steve Fetter and Frank Von Hippel, "The Hazard from Plutonium Dispersal by Nuclear-Warhead Accidents," *Science and Global Security* 2, no. 1 (1990; available at http://www.princeton.edu/~globsec/publications/pdf/2_1Fetter.pdf as of 3 January 2006).

[128] See, for example, discussion in Serber, *The Los Alamos Primer*, pp. 38-46.

[129] As Serber points out, the yield is roughly proportional to Δ^3, where Δ is the difference between the critical radius and the actual radius of the supercritical system. Since the mass is proportional to the cube of the radius, this means that the yield is roughly proportional to $(M^{1/3}/M_c^{1/3}-1)^3$, where M is the mass of material in the bomb and M_c is the minimum critical mass of that material in that state. Serber, *The Los Alamos Primer*, p. 42. As the amount of material declined from two critical masses to 1.5, the yield would decrease by a factor of 6. I am grateful to Marvin Miller for elucidating this point to me. Personal communication, January 2007.

both the nuclear material and the reflector equally (or there is no reflector), critical mass declines as the square of the material density. Hence, if the bare-sphere critical mass of weapon-grade plutonium metal in the medium-density delta phase is of the order of 16 kilograms,[130] implosion that successfully doubled the density would decrease the critical mass to 4 kilograms; implosion that tripled the density would decrease the critical mass to 1.8 kilograms. The degree of compression that can be achieved depends on the speed and sophistication of the explosive design used. With the use of a reflector, the critical mass at any given density could be significantly less. (Of course, a significant nuclear yield requires that the mass be substantially supercritical, not just critical.) One unclassified estimate suggests that with high-speed explosives in a sophisticated design, a 1-kiloton yield could be obtained from 1 kilogram of plutonium, or 2.5 kilograms of HEU.[131]

Terrorists making their first bomb, however, would be highly unlikely to be able to use such small amounts of material. For that purpose, the six kilograms of plutonium used in the Nagasaki bomb[132] is probably a reasonable estimate of the required quantity; allowing for process losses of perhaps 25% in manufacturing a bomb, a reasonable total is roughly 7.5 kilograms, just below the IAEA "significant quantity" figure of eight kilograms of plutonium.[133] The bare-sphere critical mass for 93% enriched HEU is roughly three times that for delta-phase weapon-grade plutonium,[134] suggesting a figure three times as high for an HEU implosion bomb – 18 kilograms of weapon-grade HEU, or some 22.5 kilograms when process losses are included (again, just below the IAEA significant quantity figure, which is 25 kilograms of U-235 contained in HEU).[135]

The risk of nuclear terrorism resulting from a successful theft do not decline to zero for facilities with less material than these figures, both because bombs can be made from somewhat less material (at the price of reduced yield or a requirement for more sophistication), and because there is the possibility of theft from more than one facility. Clearly, however, organizing multiple thefts would be more difficult than organizing a single theft, and it seems likely that the difficulty and risk of failure would increase sharply with the number of thefts required to achieve the objective: two thefts would be more than twice as

---

[130] H.C. Paxton and N.L. Pruvost, *Critical Dimensions of Systems Containing 235U, 239Pu, and 233U: 1986 Revision* (Los Alamos, N.M.: Los Alamos National Laboratory, 1987; available at http://www.fas.org/sgp/othergov/doe/lanl/lib-www/la-pubs/00209019.pdf as of 9 January 2007), p. 102.

[131] See Thomas Cochran and Christopher Paine, "The Amount of Plutonium and Highly-Enriched Uranium Needed for Pure Fission Nuclear Weapons" (Washington, D.C.: Natural Resources Defense Council, 13 April 1995; available at http://www.nrdc.org/nuclear/fissionw/fissionweapons.pdf as of 19 July 2005).

[132] Frank von Hippel and Edwin Lyman, "Appendix: Probabilities of Different Yields," *Science and Global Security* 4 (1993; available at http://www.princeton.edu/%7Eglobsec/publications/pdf/4_1Mark.pdf as of 5 December 2006).

[133] International Atomic Energy Agency, *IAEA Safeguards Glossary* (Vienna: IAEA, 2001; available at http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/Start.pdf as of 19 July 2005).

[134] The measured bare-sphere critical masses provided by Los Alamos are 49.1 kilograms for 93.7% enriched HEU metal, and 16.8 kilograms for delta-phase weapon-grade plutonium. See Paxton and Pruvost, *Critical Dimensions of Systems Containing 235U, 239Pu, and 233U: 1986 Revision*, pp. 97, 102.

[135] International Atomic Energy Agency, *IAEA Safeguards Glossary*.

difficult to carry off successfully than one theft (though probably less than four times as difficult).

For facilities with more than enough material for a single bomb, the risks do not simply scale linearly with the quantity of material. Clearly there is an immense difference between zero and one terrorist nuclear bombs; going from one to two terrorist nuclear bombs would make matters worse, but the difference in is substantially smaller than the leap between zero and one. Between two and three, the increase in consequences is smaller again. Moreover, terrorist ambitions are not infinite – they are likely to be looking for enough material for one or several bombs, not hundreds of bombs (and national and international responses are likely to be sufficient to prevent them from being able to get and use tens or hundreds of bombs). Hence, as DOE has pointed out, "a building with 1 ton of nuclear material in storage is as great a threat as a building with 10 tons."[136]

In the case of plutonium, the risks resulting from a successful theft would increase sharply as the quantity stolen increased from zero to 6-8 kilograms; after that, the risks would increase only modestly[137] until they took another (smaller) ramp upward when the quantity stolen reached 12-16 kilograms, enough for two bombs; and they would then proceed upward in successfully smaller steps as the quantity reached the amount needed for three, four, and more bombs. In the case of HEU, the risks resulting from a successful theft would increase sharply as the quantity stolen increased from zero to 20-25 kilograms, enough for a crude implosion bomb; they would then level out, increasing only modestly until the quantity stolen neared the amount required for a gun-type bomb, at which point they would increase again (because of the higher probability of terrorists being able to make a gun-type bomb, discussed above); and would then proceed upward in successively smaller steps as in the plutonium case. Whether the consequences of theft of enough plutonium for several implosion bombs should be considered more or less than the consequences of theft of enough HEU for one gun-type bomb is a matter of judgment – trading off the danger of terrorists gaining multiple nuclear weapons against the decreased probability they would be able to get any at all.

Clearly, reducing the risk of nuclear terrorism resulting from nuclear theft will require stringent security measures at all facilities with enough separated plutonium or HEU for a nuclear bomb. In a system for regulating security that had a large number of different security levels, facilities with enough nuclear material for several nuclear bombs would deserve still higher levels of security to keep the net risk they pose comparable to that from facilities with only enough for one nuclear bomb. But in systems with only a few gradations of security levels, such as those in use for nuclear materials in the United States and internationally, facilities or transport legs with enough nuclear material for a single nuclear bomb all deserve the highest level of security. Current thresholds for a "Category I" quantity requiring the highest levels of protection, set at 2 kilograms of plutonium or 5 kilograms of U-235

---

[136] U.S. Department of Energy, *FY 2007 Defense Nuclear Nonproliferation Budget Request*, p. 514.

[137] They would be increasing slowly rather than remaining flat until enough for a second bomb was available, because of the greater ease of making one bomb if more material was available.

contained in HEU, are appropriately conservative, and there seems little reason to advocate changing them.[138]

Implications. A fundamental point is that the risk of nuclear theft or diversion from a stockpile of plutonium or HEU is *not* closely related to the size of that stockpile. From disposition of excess plutonium to the HEU Purchase Agreement to Japan's policy of not accumulating plutonium stockpiles, a great deal of money and effort has been devoted, over the years, to policies which were targeted on reducing stockpiles that would still have tons of material remaining when the policies were fully implemented. While these policies were described as intended to reduce the risk of nuclear theft and proliferation, they would have little chance of appreciably affecting nuclear theft risks unless they eliminated the weapons-usable material entirely from particularly vulnerable buildings, which none of them are focused on doing.[139] Policies intended to reduce the risk of nuclear theft should focus on improving the security of particular vulnerable stocks (whether by improving their security where they are, or removing them to more secure locations), not on reducing the size of stockpiles that will still include many tons of material.

Material Quality and Theft Risk

Different types of nuclear material that might be stolen pose a variety of barriers to using them to make nuclear bombs; recipients with different capabilities will face varying degrees of difficulty in overcoming these barriers. In the sections below, I review a number of the key barriers posed by different types of materials. Several important previous analyses have addressed these issues;[140] the discussion below integrates (and in some cases extends, or modifies) this previous work. I begin by discussing how much more difficult the use of plutonium would be for terrorists, compared to the use of HEU.

---

[138] See, for example, International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*. These standards are not conservative by as wide a margin when one considers states as potential recipients, since states might be able to design weapons using smaller amounts of material than terrorist groups could. Even for states, however, the first bomb designs – which are the only ones for which stolen nuclear material is likely to be of much interest – are likely to require substantial quantities of nuclear material. As noted in the text, the first U.S. implosion bomb design involved 6 kilograms of plutonium; more recently, the Iraqi implosion design reportedly required some 15 kilograms of HEU. David Albright, "When Could Iran Get the Bomb?" *Bulletin of the Atomic Scientists* 62, no. 4 (July/August 2006; available at http://www.thebulletin.org/article.php?art_ofn=ja06albright as of 5 December 2006), pp. 26-33.

[139] For an extended discussion of this point in the case of plutonium disposition, see testimony of Matthew Bunn, in Subcommittee on Strategic Forces, Committee on Armed Services, *Plutonium Disposition and the U.S. Mixed Oxide Fuel Facility*, U.S. House of Representatives, 109th Congress, 2nd Session, 26 July 2006 (available at http://www.house.gov/hasc/schedules/ as of 10 August 2006).

[140] The most useful previous studies summarizing different barriers to the use of materials in weapons are those from panels of the National Academy of Sciences: U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*; U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, pp. 61-73. Other important previous analyses include "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems"; Hinton et al., *Proliferation Vulnerability Red Team Report*; U.S. Department of Energy, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*.

Plutonium vs. HEU as a Terrorist Nuclear Bomb Material

As discussed earlier, plutonium generates such a large neutron background that a gun-type device made from plutonium would be essentially guaranteed to pre-detonate, giving only a few tons to perhaps 10-20 tons of nuclear yield (depending on the specific configuration and the speed of the gun);[141] to get a yield in the kiloton range from plutonium would require an implosion device.

Working with plutonium would pose other barriers for terrorists as well. If inhaled or ingested, plutonium is far more toxic than uranium; while some members of the terrorist group may be suicidal, if the group's technical and mechanical experts are interested in their own safety, they would need to rig up at least crude glove box arrangements that would not be necessary working with uranium.[142] Plutonium is also more radioactive, modestly increasing the chance that searchers after the theft took place might be able to find the stolen items, or find a bomb as it was being smuggled into a target country. As a metal, plutonium has unusual properties that make it difficult to work with, and there are no metals with similar properties to practice on. Plutonium metal comes in several crystal phases, or allotropes: the easiest of these to work with (which is the type used in both U.S. and Russian nuclear weapons) is the delta phase, but the phase that is stable at room temperature and pressure is the alpha phase. To stabilize plutonium in the delta phase, states typically alloy it with a small percentage of gallium.[143] If terrorists got plutonium stolen from a weapons program, it might well already be alloyed with gallium; if they got civilian plutonium, however, and wanted to avoid the difficulties of working with other phases of plutonium metal, they would have to figure out how to alloy it.

These additional barriers make plutonium a somewhat less desirable material for terrorists than HEU, even if the amount of HEU available is only sufficient for an implosion-type bomb. But the vast majority of adversaries with the sophistication required to organize the acquisition of potential nuclear bomb material and make an implosion-type bomb would also be able to address the additional difficulties of working with plutonium rather than HEU. Hence, the difference in resulting probability of successful bomb-making caused by these

---

[141] For a discussion of the impacts terrorists might be able to achieve with such a plutonium gun-type weapon, see Stanislav Rodionov, "Could Terrorists Produce Low-Yield Nuclear Weapons?" in *High-Impact Terrorism: Proceedings of a Russian-American Workshop* (Washington, D.C.: National Academy Press, 2002).

[142] A reasonable glove box for handling plutonium could be made from plywood, clear plastic, and rubber gloves. See Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.4.

[143] The fact that gallium is used to stabilize plutonium in the delta phase was declassified in 1995. See item II.L.48 in U.S. Department of Energy, *Restricted Data Declassification Decisions 1946 to the Present (RDD-7)* (Washington, D.C.: DOE, 2001; available at http://www.fas.org/sgp/othergov/doe/rdd-7.html as of 14 August 2006). There are suggestions that even North Korea, perhaps the least developed state ever to have attempted to manufacture plutonium-based weapons, has alloyed its plutonium with gallium. When North Korean experts showed Siegfried Hecker a sample of their plutonium, they said it was alloyed, and that while they were not authorized to say what with, they used the same approach as the United States. See Hecker's testimony in Committee on Foreign Relations, *An Update on North Korean Nuclear Developments*, U.S. Senate, 108th Congress, 2nd Session, 21 January 2004 (available at http://www.senate.gov/~foreign/hearings/2004/hrg040121a.html as of 9 August 2006). As Hecker notes, gallium is not the only possibility for alloying plutonium to stabilize it in the delta phase; aluminum is another.

additional differences between plutonium and HEU are probably small, and I do not include a further discount for the risks of plutonium theft based on these factors.

Isotopic Barriers: Uranium

Typical "weapon-grade" uranium is enriched to 93% or more U-235. Uranium at much lower enrichments, however, can be used in nuclear weapons, and all uranium with enrichments of 20% or more U-235 is internationally defined as HEU and subject to stringent controls.[144] Making a bomb from material with enrichments below 93% poses three main problems: increased critical mass, increased risk of pre-initiation (making it more difficult to make a gun-type bomb) and decreased yield.

Increased Critical Mass

The more the U-235 is diluted with U-238, the more material is required to make a nuclear bomb. With larger amounts of material needed, the problems of getting sufficient material and making it into a gun-type bomb increase. Figure 4.5 shows the critical mass of a uranium metal sphere with a 10-cm beryllium reflector as a function of enrichment. As can be seen, the curve is fairly flat from roughly 40% enrichment to 93% enrichment. The critical mass at 93% is 14.9 kilograms, at 70% 23.7 kilograms, and at 40% 60.0 kilograms, still only four times the amount required at 93%.[145] Below 40% enrichment, however, the curve becomes quite steep. At 20%, the official dividing line for HEU, 220.7 kilograms of material would be required for a single critical mass. As can be seen, the 20% dividing line between HEU and LEU is to some extent arbitrary: in principle, it is possible to make nuclear explosives with material at less than 20% enrichment, though as far as is known it has never been done, and a very large amount of material would be required.

Systems for categorizing nuclear materials should take into account that at lower enrichments, a larger amount of material is required to have the same strategic significance. Currently, however, both U.S. domestic and international systems for categorizing nuclear material do not take enrichment levels into account, but simply consider any HEU containing at least 5 kilograms of U-235 to be a Category I quantity, requiring the highest level of protection, regardless of its enrichment.[146] By contrast, the IAEA safeguards system already includes the concept of an "effective kilogram," defined, in the case of enriched uranium, as its weight in kilograms multiplied by the square of its enrichment.[147] If this method were used

---

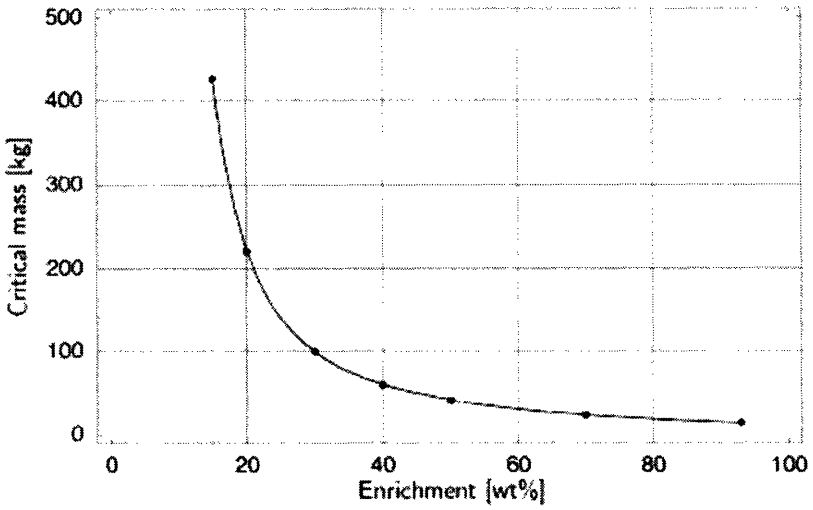
[144] International Atomic Energy Agency, *IAEA Safeguards Glossary*, p. 26.

[145] Alexander Glaser, then of the Massachusetts Institute of Technology, personal communication, September 2002. Similarly, measurements at Los Alamos indicate that a 93.6% enriched uranium metal sphere at 18.6 g/cm^3 density with a slightly thicker beryllium reflector (11.8 cm) would have a modestly lower critical mass, 13.1 kilograms. See Paxton and Pruvost, *Critical Dimensions of Systems Containing 235U, 239Pu, and 233U: 1986 Revision*, p. 97. Similar ratios for different enrichments apply for bare spheres.

[146] See, for example, International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*.

[147] See the definition in paragraph 104 of *The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons*, INFCIRC/153 (Corrected) (Vienna: International Atomic Energy Agency, 1972; available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf153.shtml as of 22 August 2005).

Figure 4.5: Enrichment and Critical Mass for a Reflected Uranium Sphere



Critical mass of a uranium sphere with a 10 centimeter thick beryllium reflector. MCNP 4B calculations at 300 degrees K. Assumed uranium density 19 g/cm^3.

Source: Alexander Glaser, "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Levels," *Science and Global Security* 14, 2006, pp. 1-24.

to define the 5-kilogram physical protection threshold, then, for example, 5.8 kilograms of 93% enriched HEU would be a Category I quantity, but it would take 31.2 kilograms of 40% enriched material to be a Category I quantity – a 5-1 ratio, similar to the 4-1 ratio of the critical masses at these enrichment levels. Alternatively, a more precise relation between enrichment level and the quantity of material required for a bomb could be used.[148]

Increased Risk of Pre-Initiation

The much larger total quantity of material required for a gun-type bomb made with lower-enrichment HEU means that there is far more material that might release a neutron that would start the chain reaction prematurely. Each kilogram of U-235 undergoes 0.0056 spontaneous fissions per second, while each kilogram of U-238 undergoes 6.78 fissions per second, a rate over 1200 times higher.[149] In material with such high concentrations of U-235, the neutron background is so low that neutrons from α-*n* reactions may be significant, if light-element impurities are present in the metal, as is often the case. In particular, as the alpha-emitter U-234 is also concentrated in the process of uranium enrichment, weapon-grade uranium might contain something like 1% U-234, and if the metal contained 0.2% oxygen atoms, the U-234 in one kilogram of such HEU would cause the release of 0.56 additional

[148] Glaser has found, for example, that the data from his simulations of critical mass for spheres with 10-cm reflectors can be well approximated with an equation based on enrichment ("x") expressed as the weight percent of U-235 (e.g., 20, 50, 90): critical mass=1.0535E6 (x^{-3}) - 8309 (x^{-2}) + 2453 (x^{-1}) - 12.3265. Personal communication, September 2002.

[149] See, for example, Glaser, "Proliferation Potential of Uranium Fuel."

neutrons/second.[150] Hence, 50 kilograms of 93% enriched HEU, as might be used for a gun-type bomb, would emit approximately 75 neutrons per second, on average. At 70% enrichment, with a bare sphere critical mass in the range of 85 kilograms, that mass would emit some 350 neutrons per second, while at 45% enrichment, with a bare sphere critical mass in the range of 185 kilograms, that mass would emit nearly 1400 neutrons per second. In each of these cases, essentially all of the neutrons are coming from the U-238, so the neutron generation is directly proportional to the total quantity of U-238 present.[151]

With this larger neutron background, the probability of successfully assembling a gun-type device to optimum criticality without pre-initiation declines. If one assumes an assembly time of 1 millisecond, the probability that no spontaneous fissions will occur during that time is over 97% for 93% enriched weapon-grade HEU; over 80% for 70% enriched material; but only 50% for 45% enriched material.[152] While not every neutron will succeed in initiating a chain reaction,[153] the chance of a chain reaction beginning prematurely increases significantly with decreasing enrichment. The increase in the risk of pre-detonation in a gun-type device with reduced enrichment is likely to be even more substantial than these figures suggest, as with larger critical masses, the distance to be traveled while the system is in a critical state – and therefore the assembly time for a given speed – will increase. Moreover, high speeds will require larger guns as the quantity of material increases.[154]

Decreased Explosive Yield

Lower enrichments will also result in lower explosive yields, other things being equal. The explosive yield of a fission bomb is determined by how many fissions take place between the time the chain reaction begins and the time the assembly expands enough that it is no longer critical, shutting off the chain reaction. Hence, the yield is very sensitive to the neutron multiplication rate, often denoted as α.[155]

---

[150] See Steve Fetter et al., "Detecting Nuclear Warheads," *Science and Global Security* 1 (1990; available at http://www.princeton.edu/~globsec/publications/pdf/1_3-4FetterB.pdf as of 13 August 2006), p. 229. Cosmic rays also create some neutron background, but this is at a much lower rate and does not substantially affect the overall probability of pre-initiation even in weapon-grade uranium; in less enriched uranium, both the cosmic ray neutrons and the α-*n* neutrons are dominated by the neutrons from spontaneous fission in U-238.

[151] Critical masses in this paragraph are rounded from Glaser, "Proliferation Potential of Uranium Fuel."

[152] Glaser, "Proliferation Potential of Uranium Fuel."

[153] For a discussion of the odds of a neutron starting a chain reaction – which depend on how critical the system is – see Serber, *The Los Alamos Primer*, pp. 46-49.

[154] Serber argues that the required gun mass is roughly proportional to the shell mass and "very roughly" to the cube of the of required shell velocity, but this was based on rather preliminary reviews of gun ballistics. See Serber, *The Los Alamos Primer*, p. 56.

[155] Serber uses the notation $(\nu'-1)/\tau$ for α (the latter notation not yet having been invented), where ν' is the effective neutron number – the net number of neutrons resulting from each fission, taking into account losses and absorption, and τ is the mean neutron lifetime in the system. Thus α reflects both how much the number of neutrons increases with each generation of fission, and how rapidly these generations occur.

Serber derives an approximate expression which indicates that the efficiency of a device is proportional to the following factors:[156]

$$f \propto \frac{\alpha^2}{\varepsilon} R^2_{co} \Delta^3$$

In this formulation, f is the efficiency (the fraction of the total fissionable material that is fissioned, which itself is proportional to the yield), α describes the effective neutron multiplication rate in the system's initial state, ε is the fission energy released per unit mass of fissionable material, R_{co} is the radius at which the system in its initial state was critical, and Δ is the "excess radius," that is, the difference in radius between a just-critical mass in the system's initial state and the actual radius in the initial state, a measure of the initial supercriticality of the system. (As this expression is a very approximate one worked out in 1943, it has not been measured precisely over the full range of possible enrichments that might be used in a bomb, but it is sufficient for providing a general idea of the effect of declining enrichment.)

Reduced enrichments reduce α, because collisions with U-238 atoms reduce the energy of many of the neutrons below the point where they can cause fissions.[157] Indeed, the initial value of alpha for a supercritical system of two bare-sphere critical masses declines linearly with decreasing enrichment.[158] Since the yield is proportional to α^2, and α declines linearly with enrichment, one might expect that yield would decline with the square of enrichment. But the relationship is more complex than this, because at lower enrichments, R_{co} and Δ are both somewhat larger, because of the increased masses required. Overall, however, yield is sharply reduced with decreasing enrichment. By one estimate, the yield of a gun-type bomb assembling two critical masses of 36% enriched HEU would be roughly an order of magnitude less than that a system assembling two critical masses of 93% enriched HEU, even assuming no predetonation.[159] Similarly, in an implosion bomb, it is unlikely to be possible to achieve as large a criticality insertion with the large amount of material that would be used at 36% as it would be possible to achieve with 93% material, significantly reducing yield.

Uranium Isotopic Barriers: Summary

Clearly, less enriched material poses a variety of difficulties for potential terrorist bomb-makers. As already discussed, approaches to specifying the minimum amount of material requiring high levels of security should take into account the larger quantities of material needed for a bomb at lower enrichments, which they do not currently do. The increased neutron background at lower enrichments could make it difficult to make a gun-type bomb, but is not enough to significantly complicate use of these materials in an implosion-type bomb. As a result, for enrichments in the 20-40% range, estimates of the probability that adversaries could make a bomb from the stolen material should be based on use of it in an

---

[156] See Serber, *The Los Alamos Primer*, p. 42.
[157] Serber, *The Los Alamos Primer*, pp. 21-22.
[158] See Glaser, "Proliferation Potential of Uranium Fuel."
[159] This result is based on simplified simulations. Calculations provided by Michael Levi, personal communication, June 2006.

implosion-type bomb, not in a gun-type bomb; even at enrichments in the 40-60% range, terrorists may choose to attempt an implosion bomb. The reduced yield resulting from using lower enrichments would reduce casualties and direct economic damage from a terrorist nuclear blast, but would not prevent the terrorists from achieving kiloton-range yields, which would still have immense consequences. Overall, the probability that terrorists could get a significant nuclear yield out of enough HEU for a gun-type bomb would not be greatly reduced as the enrichment fell from 93% to 50% or so; for enrichments in the 20-40% range, the 0.6 discount factor for implosion-type bombs should be used, along with some additional discount factor for the reduced yield and other complications associated with such low enrichments.

An analysis by experts from the national laboratories provides a useful summary of the barriers to making weapons from different types of HEU. They characterized the barriers to making a bomb from HEU with enrichment of 80% or above as "insignificant"; the barriers for enrichments between 50% and 80% as "insignificant (+)"; the barriers for enrichments of 35% to 50% as "low (+)"; and the barriers for 20-35% enriched material as "medium."[160]

Isotopic Barriers: Plutonium

Unlike uranium, all isotopes of plutonium can sustain an explosive fast-neutron chain reaction. Different isotopes of plutonium, however, generate quite different levels of neutrons, heat, and other radiation, posing a variety of difficulties for potential bomb-makers.

The most desirable isotope for weapons use is Pu-239, formed when U-238 absorbs a neutron; it generates less heat than most other plutonium isotopes and fewer neutrons than any of them. As nuclear fuel continues to be irradiated, some of the Pu-239 absorbs additional neutrons and forms Pu-240, which is problematic because of the large number of background neutrons resulting from its high rate of spontaneous fission. Over time, small amounts of Pu-241, Pu-242, and Pu-238 also begin to accumulate. Table 4.5 outlines the relevant properties of the key plutonium isotopes; Am-241, the decay product of Pu-241, is also included, as the heat and gamma rays it generates can be important in some cases.

Plutonium produced specifically for weapons purposes is typically irradiated in reactors to relatively low burn-ups and hence typically contains in the range of 93% Pu-239 and 7% Pu-240. As far as is known, all the nuclear weapons that any state has actually incorporated into its arsenal have been made from such "weapon-grade" plutonium. Plutonium that is even better than this – such as the first plutonium produced in the Manhattan Project, used in the Nagasaki bomb – is sometimes referred to as "super-grade." Plutonium with Pu-240 contents in the range of 7-18 percent is often referred to as "fuel-grade," while plutonium with Pu-240 content in the range of 18-30 percent, typical of commercial operation of light-water reactors is often referred to as "reactor-grade." When plutonium is reprocessed and recycled as mixed-oxide (MOX) fuel, so that the plutonium is irradiated a second time, further undesirable isotopes build up; plutonium from MOX spent fuel is sometimes referred

[160] "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," p. 11.

Table 4.5: Key Properties of Plutonium Isotopes

Isotope	Critical Mass (kg)	Half Life (years)	Decay Heat (watts/kg)	Neutron Generation (neutrons/g-sec)
Pu-238	10	88	560	2600
Pu-239	10	24,000	1.9	0.02
Pu-240	40	6,600	6.8	900
Pu-241	13	14	4.2	0.05
Pu-242	89	380,000	0.1	1700
Am-241	57	430	110	1.2

Source: "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems" in *Technological Opportunities to Increase the Proliferation Resistance of Global Nuclear Power Systems (TOPS)* (Washington, D.C.: U.S. Department of Energy, Nuclear Energy Research Advisory Committee, 2000, available at http://www.nuclear.gov/nerac/FinalTOPSRptAnnex.pdf as of 9 January 2007), p. 4.

to as "MOX grade."[161] The plutonium produced in the breeding blankets of a fast-breeder reactor (FBR) is typically better than weapon-grade. Table 4.6 shows the isotopic content of different grades of plutonium. The table shows two burnup levels for reactor-grade plutonium, 33 gigawatt-days/ton (GWd/t) and 50 GWd/t. The MOX grade plutonium referred to in the table comes from MOX made from reactor-grade plutonium at 33 GWd/t, which is then irradiated again to 33 GWd/t.

Despite the terms "weapon-grade" and "reactor-grade," all of these grades are usable in nuclear weapons. The barriers of increased neutron generation, heat, and radiation can all be overcome to varying degrees, with varying degrees of sophistication. Table 4.7 shows the critical masses, neutron generation, and heat generation for the different grades of plutonium.

Increased Risk of Pre-Initiation

A key difficulty in using reactor-grade or MOX-grade plutonium rather than weapon-grade plutonium in a bomb is the increased neutron background, which increases the chance that the chain reaction will begin sooner than intended, reducing the explosive yield. If reactor-grade plutonium was used in a simple design like the Nagasaki bomb, featuring a solid ball of plutonium surrounded by tamper and explosives, there would be more than a 90% chance of some degree of pre-initiation.[162]

But it is important to understand that in a system similar to the Nagasaki bomb (that is, with roughly the same design and amount of plutonium), the "fizzle yield" – the yield if a neutron starts the chain reaction at the worst possible moment, when the system first becomes critical – is still in the range of a kiloton.[163] No matter how many neutrons are present, it is

[161] For discussions of these different grades of plutonium, see, for example, Bruno Pellaud, "Proliferation Aspects of Plutonium Recycling," *Journal of Nuclear Materials Management* 31, no. 1 (Fall 2002; available at http://www.inmm.org/topics/contents/fall02issue/pellaud.pdf as of 4 August 2006).
[162] Mark, "Explosive Properties of Reactor-Grade Plutonium."
[163] For discussions, see U.S. Department of Energy, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*, pp. 37-39; U.S. National

Table 4.6: Isotopic Contents of Different Plutonium Grades

Grade	Pu-238	Pu-239	Pu-240	Pu-241	Pu-242	Am-241
Super-grade	0	0.98	0.02	0	0	0
Weapon-grade	0.0001	0.938	0.058	0.0013	0.0002	0.0022
Fuel-grade	0.012	0.709	0.154	0.0636	0.019	0.0424
Reactor-grade (33 GWd/t)	0.013	0.603	0.243	0.056	0.05	0.035
Reactor-grade (50 GWd/t)	0.027	0.47	0.26	0.09	0.09	0.06
MOX-grade	0.019	0.404	0.321	0.107	0.078	0.0712
FBR blanket	0	0.96	0.04	0	0	0

Source: Figures for weapon-grade and reactor-grade plutonium at an exposure of 33 gigawatt-days/ton (GWd/t) are from U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options* (Washington, D.C.: National Academy Press, 1995, available at http://books.nap.edu/html/plutonium/0309051452.pdf as of 9 January 2007), p. 45. That panel was adapting figures from J. Carson Mark, by including the decay of Pu-241 to Am-241, assuming that the weapon-grade plutonium in question was 20 years old and the reactor-grade plutonium was 10 years old. Figures for super-grade plutonium and blankets from fast-breeder reactors ("FBR blankets" in the table) are from the same source the Academy panel was drawing from, J. Carson Mark, "Explosive Properties of Reactor-Grade Plutonium," *Science and Global Security* 4, 1993, pp. 111-128 (available at http://www.princeton.edu/~globsec/publications/pdf/4_1Mark.pdf as of 9 January 2007 Figures for fuel-grade plutonium are from Alexander Glaser, "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Levels," *Science and Global Security* 14, 2006, pp. 1-24.

impossible to do worse than this. The destructive radius from a one-kiloton blast would be about one-third that of the Hiroshima bomb, making such a bomb "a potentially fearsome explosive."[164]

At the other end of the spectrum of sophistication, it is an unclassified fact that some weapon designs are "pre-initiation proof" – that is their yield is not sensitive to initiation earlier than the planned time.[165] The presence of large neutron backgrounds would not make these weapons less reliable or reduce their yield.

Increased Heat

Another problem posed by using reactor-grade plutonium rather than weapon-grade plutonium is the increased radioactive decay heat generated by the reactor-grade plutonium. Six kilograms of weapon-grade plutonium (the amount discussed above as being suitable for a crude implosion bomb) would generate 15 watts of heat, while a comparable amount of reactor-grade plutonium (7.6 kilograms, taking into account the increased critical mass of this material) would generate almost 110 watts of heat, more than seven times as much. This increased heat can affect the stability and performance of the bomb's components. With this

---

Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, pp. 32-33; Mark, "Explosive Properties of Reactor-Grade Plutonium."

[164] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, p. 33.

[165] See item B.2.k in U.S. Department of Energy, *RDD-7*.

Table 4.7: Key Properties of Different Grades of Plutonium

Grade	Critical Mass (kg)	Neutrons /g-sec	Heat (W/kg)
Super-grade	n.a.	18	2.0
Weapon-grade	11.5	53	2.5
Fuel-grade	13.2	202	14.1
Reactor-grade (33 GWd/t)	14.6	338	14.4
Reactor-grade (50 GWd/t)	n.a.	457	25.1
MOX-grade	n.a.	471	22.2
FBR blanket	n.a.	36	2.1

Source: Neutron and heat generation are calculated from the isotopic properties and the contents of the different grades presented in the previous tables. Critical masses are for bare spheres of alpha-phase plutonium with a density of 19 g/cc, presented in Alexander Glaser, "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Levels," *Science and Global Security* 14, 2006, pp. 1-24. Since critical mass declines with the square of density, delta-phase plutonium, with a density in the range of 15.8 g/cc, would have critical masses some 45% higher.

much heat being generated in a Nagasaki-type design, with the insulating tamper and explosives wrapped around the pit, the temperature would rise to an equilibrium temperature in the range of 190° C.[166]

There are a variety of more and less sophisticated ways to manage the heat generated in the core of a nuclear bomb, however. As one example, it is an unclassified fact that even some of the earliest and simplest U.S. weapon designs used "insertable nuclear components" – that is, the nuclear material core was not put into the bomb until the bomb was being readied for use. A bomb core made from reactor-grade plutonium could simply be kept in a small refrigerator until the bomb was ready to be used.[167] A variety of other approaches to heat management are possible, including providing heat-transfer channels through the insulating explosives.[168]

Some analysts have argued that there is a threshold at around 2% by weight Pu-238, beyond which the plutonium is "practically unusable" in nuclear explosives.[169] This is clearly incorrect. As shown in Table 4.7, reactor-grade plutonium with an exposure of 50 GWd/t, which has a Pu-238 content of 2.7%, does generate 75% more heat than the reactor-grade plutonium with an exposure of 33 GWd/t, which has roughly half as much Pu-238. But the

---

[166] See Mark, "Explosive Properties of Reactor-Grade Plutonium."

[167] The specific heat of plutonium is 0.13 J/g°C. Therefore heating a 7.6 kilogram mass of plutonium by, say, 50 °C would require 4.9×10^4 J. If the mass were generating 110 watts of heat, it would take over seven minutes to heat up by this amount even if it were perfectly insulated after being inserted into the bomb. Adversaries attempting to use this approach would presumably detonate their bomb immediately (probably in far less than seven minutes) once insertion of the plutonium component was completed, to avoid phase changes in the plutonium. If inserting the component was expected to take a substantial time, it might be desirable to have a fan blowing cool air on the component until its insertion was completed.

[168] For brief mentions of such heat channels, see Mark, "Explosive Properties of Reactor-Grade Plutonium"; U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, pp. 32-33. Further details on heat management are classified.

[169] See, for example, Pellaud, "Proliferation Aspects of Plutonium Recycling."

heat generation, at 25 watts per kilogram, is still at a level that could readily be managed by storing the plutonium component in a refrigerator until needed, and possibly by other methods such as heat channels. There is clearly no threshold at 2% Pu-238, though it does seem clear that the difficulties of heat management will increase as the proportion of Pu-238 increases.

Increased Radiation

Reactor-grade plutonium also generates more radiation than weapon-grade plutonium does, meaning that "more shielding and greater precautions to protect personnel" – or acceptance of greater radiation doses by the personnel – "might be necessary when building and handling nuclear explosives made from reactor-grade plutonium."[170] The surface dose rate from a several-kilogram sphere of reactor-grade plutonium could be roughly 15-20 times the dose rate from a comparable sphere of weapon-grade plutonium.[171] The increased precautions required, however, are comparatively modest and easily within the capabilities of any terrorist group able to make an implosion bomb in the first place, or of any state; terrorist groups, in any case, might be willing to simply accept higher radiation doses to their personnel.

Increased Critical Mass

Unlike uranium, the increase in the critical mass as the isotopic mixture changes is comparatively modest, as shown in Table 4.5. The critical mass of reactor-grade plutonium is about one-quarter larger than that of weapon-grade plutonium and still only a fraction of the critical mass of weapon-grade uranium.[172]

Reduced Yield

Even without preinitiation, a weapon made from reactor-grade plutonium would have somewhat reduced yield compared to a similar design using weapon-grade plutonium, because the Pu-240 has a lower fission cross section (and higher absorption cross section) in a fast spectrum, reducing the effective neutron multiplication rate in the system. Unlike the uranium case, however, the effect is not large, as Pu-240, unlike U-238, is a nuclear explosive material itself, capable of sustaining a fast-neutron chain reaction.[173]

---

[170] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, p. 33.

[171] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 45. The panel's estimates of surface dose rates are 0.94 rem/hr for weapon-grade plutonium and 15 rem/hr for reactor-grade plutonium (aged for 10 years after separation), but it does not appear from their discussion that they have included an increased quantity of material for the reactor-grade plutonium; the factor of 20 in the text includes increasing the amount of plutonium present by the ratio of the critical masses.

[172] Similarly, the Los Alamos measured data indicate a bare-sphere critical mass for delta-phase metal containing only 4.5% Pu-240 (weapon-grade) of 16.8 kilograms, and a comparable critical mass for plutonium containing 20.1% Pu-240 (low-burnup reactor-grade) of 19.3 kilograms, only 15% higher. See Paxton and Pruvost, *Critical Dimensions of Systems Containing 235U, 239Pu, and 233U: 1986 Revision*, p. 102.

[173] This is why the graph of yield vs. fissile content presented by Pellaud is completely incorrect. See Pellaud, "Proliferation Aspects of Plutonium Recycling."

Increased Detectability

Plutonium is much easier to detect than HEU; both its gamma emissions and its neutron emissions are orders of magnitude higher, significantly easing detector design, making shielding more difficult, and making detection possible at somewhat longer ranges. Reactor-grade plutonium is much more radioactive than weapon-grade plutonium (with a typical gamma dose at the surface about 15 times higher and a neutron background some seven times higher).[174] Hence, the probability that a terrorist bomb would be detected and stopped as it was heading toward its target, or that the plutonium itself would be detected and stopped as it was being moved from where it was stolen to where the bomb was to be built, or that the bomb-making operation itself would be detected, would be somewhat higher for reactor-grade plutonium. In general, however, even reactor-grade plutonium could only be detected if it was quite close to the detector – that is, if the adversaries chose to transport the material through a border crossing equipped with nuclear material detectors (which seems unlikely, since the adversaries would in general be able to observe which crossings had such detectors in place), or if those searching for the plutonium had quite precise intelligence information on where to look (which also seems unlikely).

Summary of Plutonium Isotopic Barriers

Weapon-grade plutonium is generally the preferred material for making nuclear explosives. But any state or group capable of making a nuclear bomb from weapon-grade plutonium would also be capable of making a nuclear bomb from reactor-grade plutonium. And sophisticated nuclear weapon states could, if they chose, make reliable, high-yield weapons from reactor-grade plutonium (using pre-initiation-proof designs). Virtually any isotopic composition of plutonium is potentially weapons-usable.[175]

A 1997 DOE report provides the clearest official unclassified summary of the issue of using reactor-grade explosives in weapons:[176]

---

[174] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 45.

[175] The exception is plutonium containing substantial quantities of Pu-238, which generates such intense heat that it is not practical to make nuclear explosives from it; plutonium containing 80 percent or more Pu-238 is therefore exempted from international safeguards. See International Atomic Energy Agency, *IAEA Safeguards Glossary*.

[176] U.S. Department of Energy, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*, pp. 37-39. This statement was reviewed by all three U.S. nuclear weapons laboratories before publication. Similarly, Mark (who led the weapons-design team at Los Alamos for many years) concludes that "Reactor-grade plutonium with any level of irradiation is a potentially explosive material. The difficulties of developing an effective design of the most straightforward type are not appreciably greater with reactor-grade plutonium than those that have to be met for the use of weapons-grade plutonium." Mark, "Explosive Properties of Reactor-Grade Plutonium." A committee of the National Academy of Sciences reached essentially the same conclusion, after detailed classified briefings from the weapons labs. The committee included, among others, a former director of the Lawrence Livermore National Laboratory; a participant in the Manhattan Project; a Nobel Prize-winning physicist; and a physicist who did the engineering design for the first hydrogen bomb. See U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, pp. 32-33.

> The degree to which these obstacles [to using reactor-grade plutonium in weapons] can be overcome depends on the sophistication of the state or group attempting to produce a nuclear weapon. At the lowest level of sophistication, a potential proliferating state or subnational group using designs and technologies no more sophisticated than those used in first-generation nuclear weapons could build a nuclear weapon from reactor-grade plutonium that would have an assured, reliable yield of one or a few kilotons (and a probable yield significantly higher than that). At the other end of the spectrum, advanced nuclear weapon states such as the United States and Russia, using modern designs, could produce weapons from reactor-grade plutonium having reliable explosive yields, weight, and other characteristics generally comparable to those of weapons made from weapons-grade plutonium. ... Proliferating states using designs of intermediate sophistication could produce weapons with assured yields substantially higher than the kiloton range possible with a simple, first-generation nuclear device.

As a committee of the National Academy of Sciences put it: "Theft of separated plutonium, whether weapons-grade or reactor-grade, would pose a grave security risk."[177] The committee members have since had the opportunity to discuss these conclusions with weapons designers from all five of the Nonproliferation Treaty nuclear weapons states, none of whom have disagreed with the broad outlines of these conclusions.[178] Indeed, one Russian weapon-designer who had been assigned to examine what kind of nuclear explosives terrorists might be able to build pointed out to me that terrorists might actually *prefer* reactor-grade plutonium, as an implosion bomb with reactor-grade material would not require a neutron generator, avoiding one of the modestly difficult steps in making an implosion bomb.[179]

A group from the national laboratories made almost no distinction between the different grades of plutonium, summarizing the isotopic barriers to the use of weapon-grade plutonium in weapons as "low (-)," the barriers to the use of typical reactor-grade plutonium with roughly 60% Pu-239 as "low," and the barriers to use of very high burn-up reactor-grade plutonium with 40% or less Pu-239 as "low (-)" – on a scale that included "insignificant," "low," "medium," "high," and "very high."[180]

Hence, for the purposes of this dissertation, all grades of plutonium are referred to as "weapons-usable" material. The probability that a subnational group would be able to make a kiloton-range bomb from reactor-grade plutonium is only modestly lower than the probability that they could make a kiloton-range bomb from weapon-grade plutonium; considering all the

---

[177] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium*, p. 33.
[178] Personal communications from John P. Holdren and Richard L. Garwin.
[179] Personal communication, October 1996.
[180] "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," p. 11. Similarly, the National Academy study of the spent fuel standard concluded that the isotopic barrier to a terrorist group making a bomb from reactor-grade plutonium rather than weapon-grade plutonium was "low," but that this barrier would be "moderate" for a proliferant state recipient, which might have higher standards for the type of bomb it wanted to make. U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*, p. 23.

various aspects (including detectability), a reduction factor in the risks resulting from successful theft of 0.8 for reactor-grade plutonium compared to weapon-grade plutonium is probably reasonable. Nevertheless, any facility with enough plutonium for a bomb, whether weapon-grade or reactor-grade, should be considered as potentially posing high consequences of nuclear theft.[181]

Isotopic Barriers: U-233 and Other Nuclear Explosive Isotopes

As far as is known, every nuclear weapon that has ever been manufactured has been made from HEU, plutonium, or some combination of the two. However, other materials can in principle be used to make nuclear explosives.

U-233 has long been recognized as a suitable material for either nuclear weapons or nuclear fuel and is covered by IAEA safeguards and both U.S. and international physical protection guidelines.[182] In addition, some isotopes of neptunium, americium, and a few other elements are potentially usable in nuclear explosives. The relevant properties of these isotopes are shown in Table 4.8; U-235, Pu-239, and Pu-240 are also included for comparison.

Just as Pu-239 is produced by neutron absorption in U-238, U-233 is produced by neutron absorption in the main naturally occurring thorium isotope, Th-232. World resources of thorium are believed to be several times those of uranium; India, in particular, has limited uranium resources (and has been cut off from most international fuel supplies since its 1974 nuclear test, though that may now be changing), but has large thorium resources. As a result, India has long been interested in fuel cycles based on breeding U-233 from thorium. (Th-232 itself, like U-238, is not itself useful as a fuel, but only as a fertile material for producing fuel.)

Because of this production process, the world's U-233 exists primarily in forms not diluted with U-238. Pure U-233 has a bare sphere critical mass in the range of 15 kilograms, somewhat more than that of Pu-239, but far less than that of U-235. Its neutron generation is low enough that it can be used in a gun-type bomb, and its decay heat, while higher than U-235, is much lower than Pu-239. In short, it is a very attractive weapons material. On the other hand, the alpha activity of U-233, like that of all grades of plutonium, is high enough it has to be handled in a glove-box (at least for those bomb-makers who care about their long-term cancer risks), which is not required for U-235.[183] Moreover, U-233 is typically contaminated with small quantities (hundreds of parts per million) of U-232, and the thalium daughter product of U-232 decay (Tl-208) emits very penetrating gamma rays (2.6 MeV).

---

[181] This stands in stark contrast to the recommendations in Pellaud, "Proliferation Aspects of Plutonium Recycling." Pellaud is entirely wrong on several major technical points related to the usability of reactor-grade plutonium in nuclear explosives, particularly in the assertion that MOX-grade material is "practically unusable" in nuclear weapons, and should be treated for safeguards purposes like natural or depleted uranium.

[182] See, for example, International Atomic Energy Agency, *IAEA Safeguards Glossary*; International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities.*

[183] C. W. Forsberg et al., *Definition of Weapons-Usable U-233*, ORNL/TM-13517 (Oak Ridge, Tenn.: Oak Ridge National Laboratory, 1998; available at http://www.ornl.gov/sci/criticality_shielding/HopperPubs/DefWeaponsUsableU-233ORNLTM13517.pdf as of 12 August 2006), p. 15.

Workers handling typical U-233 without shielding for several hours will begin to suffer radiation sickness.[184] In a thorium-U-233 fuel cycle, however, it is possible to produce U-233 with very little U-232 by separating protactinium from the spent fuel, and allowing the dominant Pa-233 isotope to decay to U-233.[185]

Like U-235, U-233 can be diluted with U-238 to an isotopic mix that is no longer practical to use in nuclear explosives. Material with 12% U-233 has approximately the same critical mass as material with 20% U-235.[186] In 2000, DOE accepted, for its internal accounting and physical security rules, that material with less than 12% U-233 was the equivalent of LEU.[187]

Only a few countries have stockpiles of separated U-233, and in most cases these stockpiles exist at facilities that also contain larger stockpiles of HEU or separated plutonium, with the associated security. Overall, while stocks of U-233 should be heavily guarded, the small number of secure locations where kilogram quantities of this material exist make it a very small part of the global risk of nuclear theft. In the future, however, if a significant number of countries begin to pursue fuel cycles based on breeding and recycling of pure U-233, the risk from U-233 theft could increase substantially. Options are available for breeding and consuming U-233 in place without reprocessing, to a limited degree, and for recycling U-233 in an LEU form mixed with U-238; the proliferation-resistance of different proposed approaches to thorium-U-233 fuel cycles requires further examination.[188]

The other isotopes in the table are produced by successive neutron capture from either U-235 or plutonium, or, in the case of protactinium, by radioactive decay of U-235. Pa-231 is the only one of these that occurs in nature to any significant degree, at 1-3 parts per million in uranium ores.[189] It is typically produced only in gram quantities, and as far as is known, no one has ever seriously contemplated attempting to make a nuclear bomb from this very high critical-mass material. (Even with 100% efficient separations, assuming a concentration of 2 parts per million, producing a critical mass of Pa-231 would require processing over 80,000 metric tons of uranium ore, several times the amount mined worldwide in a typical year.)

---

[184] Forsberg et al., *Definition of Weapons-Usable U-233*, p. 15.
[185] Personal communication from Marvin Miller, January 2007.
[186] Forsberg et al., *Definition of Weapons-Usable U-233*.
[187] Joseph Rivers and D.L. Whaley, "Review of the Department of Energy Graded Safeguards Table," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).
[188] See, for example, International Atomic Energy Agency, *Thorium Fuel Cycle -- Potential Benefits and Challenges*, TECDOC-1460 (Vienna: IAEA, 2005; available at http://www-pub.iaea.org/MTCD/publications/PDF/TE_1450_web.pdf as of 12 August 2006); Jungmin Kang and Frank N. von Hippel, "U-232 and the Proliferation-Resistance of U-233 in Spent Fuel," *Science and Global Security* 9 (2001; available at http://www.princeton.edu/~globsec/publications/pdf/9_1kang.pdf as of 12 August 2006).
[189] For a discussion of the properties of Pa-231, the only long-lived isotope of protactinium, see Manson Benedict, Thomas H. Pigford, and Hans Wolfgang Levi, *Nuclear Chemical Engineering*, 2nd ed. (New York: McGraw-Hill, 1981), pp. 220, 420-424.

Table 4.8: Key Properties of U-233 and Alternative Nuclear Materials

Isotope	Critical Mass (kg)	Half Life (years)	Decay Heat (watts/kg)	Neutron Generation (neutrons/g-sec)
U-233	15	160,000	0.3	0.0009
U-235	50	700,000,000	0.0001	0.00001
Pu-239	10	24,000	1.9	0.02
Pu-240	40	6,600	6.8	900
Pa-231	162	32,800	1.3	0
Np-237	59	2.1×10^6	0.021	0.00014
Am-241	57	430	110	1.2
Am-242m	9-18 kg	141	n.a.	5.8×10^7
Am-243	155	7,380	6.4	.9
Cm-245	13	8,500	5.7	147
Cm-246	84	4,700	10	9×10^6
Bk-247	10	1,400	36	0
Cf-251	9	898	56	0

Source: "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems" in *Technological Opportunities to Increase the Proliferation Resistance of Global Nuclear Power Systems (TOPS)* (Washington, D.C.: U.S. Department of Energy, Nuclear Energy Research Advisory Committee, 2000, available at http://www.nuclear.gov/nerac/FinalTOPSRptAnnex.pdf as of 9 January 2007), p. 4. There is an error in the original table with respect to the neutron generation rate of U-235; that is calculated here from the data provided in "Chart of Nuclides" (Upton, N.Y.: Brookhaven National Laboratory, available at http://www.nndc.bnl.gov/chart/ as of 9 January 2007). Critical mass of Am-242m, a material left out of the original table, is from David Albright and Lauren Barbour, "Troubles Tomorrow? Separated Neptunium-237 and Americium," in *The Challegenges of Fissile Material Control,* David Albright and Kevin O'Neill, eds. (Washington, DC: Institute for Science and International Security, 1999, available at http://www.isis-online.org/publications/fmct/book/New%20chapter%205.pdf as of 9 January 2007), pp. 86-96. Half-life and neutron generation of Am-242m are from "Chart of Nuclides."

The other isotopes on the table occur in small concentrations in spent fuel. The only ones on the list that exist in substantial quantities are neptunium and americium; estimates suggest that a total of over 100 tons of neptunium and americium exist in spent fuel around the world.[190] Np-237, of these isotopes, holds the most potential for weapons applications – though DOE has declassified its judgment that the americium isotopes should also be of concern for potential weapons use.[191] The neutron generation rate of Np-237 is low enough that it could potentially be used in a gun-type bomb. Only a few countries, typically weapon states, have separated kilogram quantities of neptunium, americium, or curium, and these

[190] David Albright and Lauren Barbour, "Troubles Tomorrow? Separated Neptunium-237 and Americium," in *The Challenges of Fissile Material Control,* ed. David Albright and Kevin O'Neill (Washington, D.C.: Institute for Science and International Security, 1999; available at http://www.isis-online.org/publications/fmct/book/New%20chapter%205.pdf as of 11 January 2007).

[191] Albright and Barbour, "Separated Neptunium-237 and Americium."

stocks are typically stored at sites that also have much larger quantities of HEU or plutonium. They contribute only a tiny portion of the global risk of nuclear theft.[192] In the future, however, advanced transmutation fuel cycles might call for separation of these materials, and the risk they pose could become more important.[193] These materials are not formally included in either IAEA safeguards or international physical protection recommendations. In 1999, the IAEA Board of Governors agreed on a monitoring approach for neptunium and americium, but as of 2005, the IAEA reported that states were not providing the information on separated stocks of these materials that had been agreed, making it difficult for the agency to have enough information to sustain its previous conclusion that current stocks posed a low proliferation risk.[194] It is worth noting that the latest DOE categorizations of nuclear material, shown in Table 4.4, treat separated forms of Np-237, Am-241, and Am-243 exactly the same way that U-235 is treated – but do not include any other materials beyond the traditional plutonium, U-235, and U-233.

Mass and Size Barriers

Other things being equal, a larger and heavier object is more difficult to steal. The mass and size of the objects to be stolen can affect both the kind of equipment needed to steal them and how difficult a theft is to conceal. A small disk of HEU or plutonium metal (of which there are some 80,000 at the Institute for Physics and Power Engineering in Obninsk, Russia, for example) might easily be slipped into a pocket without anyone noticing, if adequate security and material control procedures were not in place. By contrast, an adversary would need some kind of lifting and transport equipment to carry off plutonium in a fabricated light-water-reactor fuel assembly, and the defenders would be very likely to notice such a removal while it was still in progress. In short, the size and mass of the forms of nuclear material at a facility are key elements of the "facility environment" described above, which must be considered in considering the probability of nuclear theft.

It is useful to distinguish several ranges of size and mass. Nuclear material that can be partitioned into small units that could readily be concealed as a person was going in or out of a facility pose the smallest barrier; nuclear material in forms that could readily be carried by one person but would be more difficult to conceal (objects up to a couple of tens of kilograms) pose a somewhat larger barrier; nuclear material in forms that could only be moved by several people or one person with some kind of equipment (such as a dolly or forklift) would pose the next level of difficulty (this would be true of objects weighing up to hundreds of kilograms, such as fuel assemblies); nuclear material in forms that would require some kind of crane or other lifting machinery and would require a heavier truck to drive away (1,000 kilograms or more) would pose a further level of difficulty; and, finally, nuclear

---

[192] For this reason, I believe Michael Hynes and his co-authors are wrong to highlight controls on these materials as a key first step in reducing nuclear theft risks. See Michael V. Hynes, John E. Peters, and Joel Kvitky, "Denying Armageddon," *Annals of the American Academy of Political and Social Science* 607 (September 2006).

[193] Albright and Barbour, "Separated Neptunium-237 and Americium."

[194] International Atomic Energy Agency, *Safeguards Statement for 2005* (Vienna: IAEA, 2006; available at http://www.iaea.org/OurWork/SV/Safeguards/es2005.pdf as of 12 August 2006).

material in forms that would require multiple vehicles or vehicles so large as to be difficult to acquire and highly noticeable would be the highest level of mass and size barrier.[195]

Nuclear material in forms with large mass and size can in many cases make it very difficult or impossible to keep a theft concealed, making overt theft the only realistic option. Since overt theft raises the possibility of immediate response and pursuit, this in itself reduces the risk of theft to an important degree.

In the broad range between "large enough to be hard to conceal its removal" and "so large it would take a crane and multiple or hard-to-acquire vehicles to lift it up and carry it away," however, increasing size and bulk may have only a modest effect on the probability of a successful nuclear theft. Any group attempting an outsider theft of nuclear weapons or materials is virtually certain to have researched what items it is that they are hoping to steal and to bring equipment suitable for lifting them and a vehicle appropriate for carrying them away.

Under current DOE rules, nuclear material containing less than 10% by weight Pu-239 or U-235 is no longer considered Category I material, no matter how much of it there may be, and a large part of the reason for this is the judgment – which is not expected to change in the ongoing review of DOE's nuclear material categorization system – that the large mass of dilute material that would have to be carried off to get enough plutonium or HEU for a bomb greatly reduces the risk of theft.[196] But no one would argue that nuclear weapons themselves do not deserve the highest levels of protection – yet the size and weight of many nuclear weapons are larger than the size and weight of the roughly 90 kilograms of material that would have to stolen to get 8 kilograms of plutonium from material containing 9% plutonium by weight. Even ignoring the massive multi-megaton weapons of the past, the U.S. W80 warhead, for example, is reported to weigh over 120 kilograms,[197] and the B61 bomb over 300 kilograms.[198] Virtually any modern warhead could easily be put on a dolly and wheeled to a truck to be driven off (as could also be done with containers of dilute nuclear material); the number of people and the level of sophistication required would be far less than those needed to attack a nuclear warhead facility or well-guarded nuclear material facility in the first place.[199] Similarly, while it is often argued that tactical nuclear weapons pose a greater

---

[195] This typology is based on that presented in U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 68.

[196] Joseph Rivers, U.S. Department of Energy, responses to questions at "47th Annual Meeting of the Institute for Nuclear Materials Management," Nashville, Tenn, 16-20 July 2006.

[197] Thomas B. Cochran, William M. Arkin, and Milton M. Hoenig, *Nuclear Weapons Databook: Volume I: U.S. Nuclear Forces and Capabilities* (Cambridge, Mass.: Ballinger, 1984), p. 79.

[198] Cochran, Arkin, and Hoenig, *Nuclear Weapons Databook: Volume I*, p. 65.

[199] Here, my analysis differs sharply from that in U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*, p. 24. The Academy panel argues that the concentration of weapons-usable material in the items to be stolen "is of high importance in relation to theft for a proliferant state or a subnational group, because concentration even more than individual item size determines the scale of the entire theft operation (personnel and equipment), directly affecting both the resources the thieves would need to mobilize, the time required for the acquisition operation, and the chances of their being detected and thwarted in the course of it." I argue that this conclusion does not hold over the broad range described in the text, where the resources required for the theft do not change very much with the

nuclear theft risk than strategic weapons do, in part because on average they are smaller and lighter,[200] the difference this makes in the probability of successful theft is likely to be very small; anyone planning a theft of nuclear weapons would surely bring a vehicle big enough to carry away whatever nuclear weapons they were planning to steal.

If nuclear material in dilute form were stolen, some kind of processing would be needed to produce a form of material that could be used in a bomb. The difficulties of such processing are discussed under chemical barriers, below. If the material stolen was more dilute and therefore had greater mass and size, a larger volume of material would have to be processed, possibly requiring somewhat more time and more chemicals. There would not be any very large difference in difficulty, however, between processing material that contained 11-30% by weight Pu-239 or U-235 and material that contained 9% by weight of these materials.[201] In short, DOE's 10%-weight standard for recategorizing material as Category II is unjustified and should be revised.

A key question in considering mass and size barriers – and radiological barriers, discussed below – is how easy it would be to separate the desired material from the rest. Is the nuclear material the thieves might want "readily separable" from the other material, in the words of U.S. regulations? Clearly putting plutonium in a lead can, so that the plutonium was less than 10% by weight of the total can, should not be enough to make the plutonium Category II material if the can could be easily opened and the plutonium removed. There are often debates, however, as to how "readily separable" different types of materials are. Should a mix of plutonium oxides and other oxides, in which the plutonium oxide particles were notably larger than the others, so that they might be separated with a sieve without chemical processing, be considered "readily separable"? How likely is that adversaries would know or be able to figure out that this was possible for a given package of oxides? What about materials that might be separated with a clever use of shaped-charge explosives?[202]

---

concentration of material in the items to be stolen. This range includes most of the nuclear material forms in most common use in the world.

[200] See, for example, William Potter and Nikolai Sokov, "Practical Measures to Reduce the Risks Presented by Non-Strategic Nuclear Weapons," paper presented at The Weapons of Mass Destruction Commission, Stockholm2005 (available at http://www.wmdcommission.org/files/No8.pdf as of 18 April 2005), p. 6.

[201] Here, too, my analysis differs from that in U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options.* The Academy panel puts greater emphasis on concentration levels as a barrier to recovery of sufficient material for a bomb. The analysis here is closer to that of the Proliferation Vulnerability Red Team, which states flatly that "plutonium dilution is not a significant utility barrier" (meaning "utility" as the utility of the material to potential recipients for making a bomb), seeing the penalties in increased resources and time required as quite modest. See Hinton et al., *Proliferation Vulnerability Red Team Report*, pp. 4.5, 4.8.

[202] As one example, for a discussion of how readily cans of immobilized plutonium might be separated from canisters of radioactive glass in which they were embedded, by explosives or other means – and the extended technical dispute on that subject – see U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options.*

Chemical Barriers

Plutonium and HEU exist in a wide range of chemical forms around the world, ranging from oxide powders to nitrate solutions, from alloys and mixed oxides to contaminated ash and slag from processing. Each of these chemical forms would pose somewhat different obstacles to recovery of the material for use in nuclear weapons.

Plutonium or HEU oxide – one of the most common forms of these materials other than metal – could be used directly in nuclear weapons without converting them to metal.[203] Because of the lower density of materials in oxide form, however (particularly if not packed to full crystal density, which requires special equipment), larger quantities of material would be needed, and explosive yields would be reduced. Moreover, α-n reactions with the oxygen atoms would greatly increase the neutron background; the quantity of material needed and the higher neutron background would likely make a gun-type bomb impractical. Even for an implosion bomb with weapon-grade plutonium, the probability of preinitiation would be increased significantly. Similar conclusions can be reached about other solid compounds of plutonium or HEU, such as carbides and nitrides, though the details will differ in each case.

Alternatively, the terrorists might choose to reduce oxides to metal, using one of a number of reasonably simple, openly published processes using commercially available equipment. At Los Alamos during the Manhattan Project, for example, oxides were fluorinated in furnaces smaller than 55-gallon drums and the fluorides reduced to metal in a matter of hours in desktop-sized crucibles (known as "bombs" at the time).[204] Although not unduly difficult, any such conversion from one form to another would:

- require the group to acquire an additional set of skills, this time in chemical processing;
- require the purchase of some additional equipment (particularly a specialized crucible) and materials;
- add additional time between acquisition of the material and availability of a usable bomb;
- add opportunities for mistakes to occur and problems to arise; and
- create additional opportunities for the plot to be detected and stopped.

One reasonably detailed unclassified discussion of the obstacles terrorists would face in making nuclear weapons, by several individuals with experience in nuclear weapon design, machining, and nuclear material processing, concludes that converting oxide to metal would take "a number of days" and that while the relevant chemical steps have been "described in a straightforward manner," their "conduct is most unlikely to proceed smoothly unless in the hands of someone with experience in the particular techniques involved, and even then substantial problems could arise."[205] Others have provided assessments that are similar in

---

[203] For an authoritatively declassified statement on this point, see U.S. Congress, *Nuclear Proliferation and Safeguards*, p. 32. See also discussion in Mark et al., "Can Terrorists Build Nuclear Weapons?"

[204] Richard S. Baker, Siegried S. Hecker, and Delbert R. Harbur, "Plutonium: A Wartime Nightmare but a Metallurgist's Dream," *Los Alamos Science* (Winter/Spring 1983; available at http://www.fas.org/sgp/othergov/doe/lanl/pubs/00416629.pdf as of 19 September 2006).

[205] Mark et al., "Can Terrorists Build Nuclear Weapons?"

specifics, but less skeptical in tone. The Proliferation Vulnerability Red Team, for example, a group of experts from the national laboratories formed to assess various approaches to disposition of excess plutonium, concluded that the process of converting plutonium oxide to metal would require only two process steps of low complexity, would have 90 percent or more process efficiency, would require only two people, and, with a month or so of preparation, could be accomplished in less than a week.[206] A National Academy panel, using a reference point of 0 for the chemical barrier posed by plutonium metal, rated plutonium oxide as 1 on a scale from 0-4 (suggesting that this barrier was not very substantial), while a group from the national laboratories similarly described the chemical barrier for metal as "insignificant" and that for oxides as "low."[207] Overall, it appears that a discount factor in the range of 0.8 would be appropriate when comparing the probability that sub-national recipients will be able to make a usable bomb from nuclear material in oxide rather than metal form.

In the case of mixed compounds (including uranium-plutonium mixed oxides, or MOX, a common form of these materials in industrial use, or the uranium-aluminum mixtures common in research reactor fuel), if the concentration of weapons-usable nuclear material is high, it may still be possible to make a bomb directly from the mixture (especially if the mixture is first converted to metal). The quantities of material required if such mixtures are used directly will be high, however, because of the low resulting density of the nuclear material. One U.S. government study, for example, concluded that mixed oxides containing 30% plutonium in U-238 could in principle be used directly in a bomb without separation, though the amount of material required would be roughly ten times greater than the amount required with pure plutonium (and, though the study did not estimate this effect, the resulting yield would likely be quite small, because of the low neutron multiplication rate that could be achieved in a system with such a low density of plutonium).[208]

In general, however, recipients who acquired such mixtures would probably choose to, or have to, chemically separate the plutonium or HEU before attempting to make a nuclear bomb. This would typically require chopping or cutting the material into smaller pieces, dissolving it, and then using any of a variety of separations processes (solvent extraction, ion exchange, etc.) to separate the desired material from the other materials in the solution. These kinds of separations would require more complex processes, requiring more skill and more process steps, than simple conversion from metal to oxide; the time and resources required, the potentially detectable effluents that might be created, and the opportunities for making mistakes would all be substantially higher.[209] If the group included no one with actual

---

[206] Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.6.

[207] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 67; "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," p. 12.

[208] Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, *Safeguarding a Domestic Mixed Oxide Industry against a Hypothetical Subnational Threat*, NUREG-0414 (Washington, D.C.: NRC, 1978), p. 6.9.

[209] The Proliferation Vulnerability Red Team concluded that separating plutonium (or, by analogy, uranium) from various compounds and chemical matrices, as compared to converting metal to oxide, would require substantially more process steps of greater complexity; a larger number of personnel; three months rather than

experience in such separations, there would be a substantial probability of mistakes and problems arising that could end the project, or at least take a substantial time to fix.

On the other hand, for nearly all of the forms that are in common use which thieves might steal, all the process steps required to separate the nuclear material have been openly published. Moreover, as the Proliferation Vulnerability Red Team put it, "the equipment and materials required for the processing are not unique or unusual, and could be acquired from conventional industrial supply sources."[210] The students at the Massachusetts Institute of Technology provide a demonstration that separation from a wide range of matrices does not require years of training and experience. At the end of a one-semester course in nuclear chemical engineering (for students who were otherwise studying nuclear engineering, not chemistry), the typical final exam involved presenting the students with plutonium in an unknown chemical matrix, from which they each had to design and implement a chemical separation in the laboratory. Most of the students passed this examination without undue difficulty.[211] While this involved tiny laboratory quantities of plutonium, it nevertheless suggests that the difficulty of chemically separating plutonium from a wide variety of chemical matrices should not be exaggerated.

Processing would be somewhat more difficult in the case of chemical matrices where published processes and extensive industrial experience were not available, such as separating plutonium or uranium from ceramic materials such as those proposed for immobilization of excess weapons plutonium.[212]

Such chemical processing would also raise the danger of creating a variety of effluents that might be detected, revealing the plot in progress. Dissolution in hot nitric acid, for example, would typically release nitrogen oxides into the air, though routine monitoring of environmental releases now in place would not detect these. Liquid leaks contaminated with nuclear material might occur and might be noticed. Careful planning could greatly reduce the potentially detectable signatures, however: rigging up fume hoods and fans that would discharge the air to drums filled with sand and limestone, for example, could eliminate most detectable airborne releases.[213]

Lower concentrations of nuclear material would mean that more total nuclear material would have to be processed for a bomb. While this could affect the processing time required and the quantity of materials such as acids for dissolution that would be needed, over fairly broad ranges (for example, from 30% nuclear material down to 3-5% nuclear material, which covers nearly all the kinds of mixed compounds that most commonly exist around the world),

---

one month of preparation time; and six weeks rather than less than one week of implementation time. Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.6.

[210] Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.4.

[211] Personal communication with Ken Czerwinski, the professor who gave this exam, 2000.

[212] See, for example, discussion in U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*, pp. 23-27.

[213] Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.4.

it does not appear that reduced concentration of nuclear material would significantly reduce the operation's probability of succeeding, or greatly increase its cost.[214]

Summarizing the chemical separation issue, a National Academy of Sciences panel rated the chemical barriers posed by mixed oxides and other compounds requiring dissolution and separation as a two, on a scale from zero to four.[215] That panel also argued explicitly that "most potential proliferators with the technical expertise, personnel, and the organization required to produce an operable weapon from separated plutonium—a substantial task in itself—would also be able to extract plutonium chemically from a glass log not spiked with radioactivity. Having to do so would not substantially increase the overall time and cost of building a weapon."[216] The panel clearly had a similar view of the difficulty of separating plutonium from unirradiated plutonium-uranium mixed oxides, as it recommended that not only plutonium metal but even fabricated MOX fuel, until it was inserted into a reactor, be given security comparable to the security provided for nuclear weapons themselves.[217] The national laboratories team described the barriers to chemical separation of nuclear material from forms such as MOX fuel as "medium," on a range from insignificant to high – but then added that "the range of difficulty implied by this classification [from insignificant to high] may be rather narrow. Most chemical processes involved in the separation, extraction, and refining of fissile materials are well known and available."[218] Overall, a discount factor in the range of 0.4-0.6 for the probability that sub-national recipients would be able to make a bomb from compounds requiring chemical separation, compared to the probability that they could make a bomb from HEU or plutonium metal, seems appropriate.

DOE, in its categorization system, sets a threshold for the quantity of material that must be present before the material is considered Category I that is three times as high for plutonium that is in the form of oxides or other compounds, alloys, and mixtures considered "high-grade" materials and four times as high for HEU. This approach is technically unjustified and should be modified. There will inevitably be some process losses in separating plutonium or HEU from some compound in which it might be found, but these are most unlikely to be in the range of 60-75% of the material at hand. The Proliferation Vulnerability Red Team estimated that the process efficiency of converting oxides to metal by

---

[214] As noted earlier, the Proliferation Vulnerability Red Team reached an even more sweeping conclusion on this point, arguing that even for the most dilute concentrations of plutonium they examined (0.4% by weight plutonium), "recovery of plutonium...would not be seriously complicated by the lower concentrations." See Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.5. This conclusion is in contrast, however, with that of the National Academy panel on the spent fuel standard, which argued that lower concentrations of plutonium, meaning larger quantities of material to be processed, would be a "high" barrier to sub-national groups recovering plutonium from stolen material (and a "high" barrier to the initial theft and removal of the plutonium as well). See U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*, pp. 23-27.

[215] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 67.

[216] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, pp. 225-226.

[217] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 72.

[218] "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," p. 12.

a sub-national group would likely be in the range of 90% (meaning that only 10% of the plutonium or HEU would be lost to waste), while the efficiency for separating nuclear material from a mixed oxide might be in the range of 80%.[219] Hence, it would be appropriate to multiply the quantities required for material to count as Category I material by 1.1 or 1.2, but not by three or four.

If the nuclear material to be processed were radioactive enough that the chemical processing had to be done not just in a glove box but with remotely-operated equipment, this would create a substantial additional barrier – probably a very difficult one for subnational groups to overcome. While the chemical steps required for separation would be similar, carrying these steps out remotely requires still more equipment, preparation, and time, and the presence of radioactive fission products creates more potentially detectable effluents from the processing. Most important, with remote operations, the chance of making serious mistakes increases substantially, and the difficulties of fixing those mistakes increase enormously.[220]

Radiological Barriers

The radioactivity of nuclear material to be stolen affects the ease or difficulty of the initial theft; the detectability of the material as it is being transported away and at the site where the recipients hope to process it for use in a bomb; and the difficulty of processing it. The importance of these barriers varies, depending on the level of radiation and the kinds of doses the thieves and recipients are willing to accept.

Radiological Barriers to the Initial Theft

The radiological dose that thieves would receive in the course of a theft depends on the radiological dose rate from the material to be stolen; the amount of time the theft requires; and the means of protecting themselves from these doses that the thieves choose to use.

To derive detailed estimates of the doses that thieves or processors might receive from material emitting different dose rates requires specific time-and-motion analyses of the steps they would have to take to steal and process these materials, and few of these are available in the open literature. One unclassified Los Alamos study of this kind examined scenarios for theft of irradiated HEU fuel from a research reactor. For a typical concentration of uranium in research reactor fuel, they concluded that it might take the thieves half an hour to pull the assemblies they needed for one bomb's worth of HEU from the pool at the research reactor and carry them out to a waiting truck; that if they simply carried the radioactive assemblies by hand, they might accumulate radiation doses in their bodies at roughly twice the rate of the radiation dose at one meter; and that therefore the thieves would receive a dose roughly equivalent to the dose rate at one meter being emitted by the irradiated fuel (divided by the number of thieves among whom the work of carrying out the fuel assemblies was divided).

---

[219] Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.6.

[220] Similarly, the National Academy panel on reactor-related options for plutonium disposition concluded that remote operation would "greatly increase the difficulty" of chemical processing, increasing the chemical barrier from two to four on its 0-4 scale U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 67.

Hence, if five thieves split up the job, and the material was emitting 100 rem/hr at one meter, they would each receive a dose of roughly 20 rem.[221] Such doses would typically not cause any outward symptoms.

What dose rate is enough to protect material from theft – to make it "self-protecting" in the parlance of physical protection rules – varies by many orders of magnitude depending on the attitude of the thieves. People who want to avoid getting doses beyond current safety limits would be deterred from handling material emitting even a few rem/hr at one meter. At the other end of the spectrum, to disable a truly suicidal thief would require a huge radiation dose. While a radiation dose of 400-500 rem will kill 50% of those who receive it over the next several weeks, to be acutely disabling requires a dose in the range of 2,500-10,000 rem.[222] To deliver such a dose before the theft could be completed would require dose rates of thousands of rem/hr at one meter. The Proliferation Vulnerability Red Team summed up the situation as follows:[223]

> Dose rates of up to a few hundred rem per hour will not pose an accessibility barrier for any thief willing to expose himself to some element of danger. Dose rates in the range of a few hundred to several thousand rem per hour may not pose an accessibility barrier to those willing to take a dose of several rem to accomplish the theft. Dose rates of many thousands of rem per hour and above deliver lethal doses that will incapacitate during a theft and pose a significant accessibility barrier to all, thereby forcing shielding and remote handling during the theft and requiring the use of heavy, cumbersome equipment.

As the 9/11 attacks highlighted the dangers posed by attackers for whom their own death is part of the plan, Oak Ridge National Laboratory recently recommended that DOE's standard for "self-protecting" nuclear material be increased 100-fold, from 100 rem/hr at one meter to 10,000 rem/hr at one meter.[224] As far as current officials can determine, the 100 rem/hr standard – now enshrined not only in U.S. regulations but in physical protection convention and IAEA recommendations – was set in the 1950s, on the basis of safety, not security.[225] A strong case can be made that against terrorists unconcerned for their own safety, material emitting 100-300 rem/hr at one meter would pose little more barrier to the initial theft than would unirradiated material. Such radiation levels, however, would require

---

[221] Koelling and Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II.*

[222] For a very detailed recent discussion of this point, with an estimated model of the degree of incapacitation as a function of dose (beginning with a roughly 60 percent acute reduction in personnel effectiveness after a dose of 2,500 rem), see C.W. Coates et al., "Radiation Effects on Personnel Performance Capability and a Summary of Dose Levels for Spent Research Reactor Fuels," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July* (Northbrook, Ill.: INMM, 2006). For earlier discussions suggesting disabling doses in the range of thousands of rem, see, for example, Hinton et al., *Proliferation Vulnerability Red Team Report*, pp. 4.10-14.11; Koelling and Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II.*

[223] Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.12.

[224] Rivers and Whaley, "Review of the Department of Energy Graded Safeguards Table." For a discussion of the Oak Ridge analysis that led to this recommendation, see Coates et al., "Radiation Effects on Personnel Performance."

[225] Rivers and Whaley, "Review of the Department of Energy Graded Safeguards Table."

those orchestrating a theft to recruit people who were unconcerned about their own safety, which might limit the pool of available individuals with appropriate skills somewhat. Thieves participating for money rather than because of jihadi fervor, for example, may not be willing to steal such material.

Radiological Contributions to Post-Theft Detectability

Even if a theft were detected quickly and responders were able to get a combination of road-based and airborne radiation detection equipment to the area to search within an hour or two, there would be little chance of detecting a truck carrying unirradiated HEU: at any distance much beyond the boundaries of the truck, there would simply be no signal above background to detect. But if, instead, the truck was carrying irradiated material, there would be a much stronger potentially detectable signal. This would increase the probability that the terrorists would be found and caught; how *much* that probability would change would depend on the particular scenario (and in most cases a realistic assessment of the probability of detection would remain quite small).[226] Similarly, if the recipients have to process somewhat radioactive material, the probability that searchers might detect the building where they were doing so by its radiation signature would increase somewhat. That probability would increase still further if some volatile fission products were released in the course of processing the material, and the recipients had not taken appropriate care to limit such releases (such as with the system of fans discharging into sand and limestone described above). If the responders had good intelligence and knew where to look, these factors might have a substantial effect on the probability of the conspiracy being found and stopped; if, however, the responders did not know where to look, or were unaware that a theft had occurred and a bomb plot was underway, the probability of detecting such radiation signatures would be very low.

---

[226] Despite the strength of a radioactive source emitting 100 rem/hr at 1 meter, it might be difficult to detect a vehicle carrying such material at long distances, because of the background gamma radiation at similar energies, and the attenuation of gamma rays by air. One estimate indicates that the likely detection range for a sodium-iodide detector, given these factors, would not be likely to be more than 0.5-1.0 km. (Steve Fetter, personal communication, November 2006, using methods described in Fetter et al., "Detecting Nuclear Warheads.") An aircraft flying at 200 km/hr (so as to have reasonably long integration times, to achieve such a detector range), at an altitude of 500 m, would be able to search 0-350 km^2/hr. If we assume that the plane takes only one hour to arrive after the theft, and that the thieves spend much of their time off easily-searched major highways and hence are able to disperse into a search area whose radius grows only at 20 km/hr, then by the time the aircraft arrived the search area would already be over 1200 km^2 and expanding rapidly, giving the aircraft very little chance of finding the thieves without some intelligence on where to look. Under current circumstances in the United States, arrival of the search aircraft within one hour is a very generous assumption, as the only suitable search aircraft are located at Nellis Air Force Base in Nevada and Andrews Air Force Base in Maryland. General Accounting Office U.S. Congress, *Combating Nuclear Terrorism: Federal Efforts to Respond to Nuclear and Radiological Threats and to Protect Emergency Response Capabilities Could Be Strengthened*, GAO-06-1015 (Washington, D.C.: GAO, 2006; available at http://www.gao.gov/new.items/d061015.pdf as of 20 November 2006). The United States is almost certainly better prepared for carrying out such rapid searches than most other countries are. In short, it is not a good idea to rely on the ability to detect the fleeing vehicle carrying irradiated fuel from the air as a key contribution to prevention of theft of such fuel.

Radiological Barriers to Processing

Estimating what dose rates would pose which barriers to processing is difficult, as it depends on a complex interaction between the types of processing needed and the time they would take; the types of simple shielding the recipients might use; and the doses the recipients are willing to put up with. For example, even if a subnational group has little difficulty recruiting suicidal armed attackers to steal nuclear material, it may be far more difficult to recruit people with the expertise needed for processing nuclear material who are also willing to absorb potentially fatal radiation doses. Moreover, in most cases the chemical processing will take much longer than the initial theft will, meaning that there will be more time for large radiation doses to accumulate. Hence, in some cases a radiation level that posed only a modest barrier to the initial theft could lead the recipients to conclude that they had to shift toward remote operations for the processing, with all the complications and difficulties that remote operations would raise. Careful assessments of the radiation levels that would force adversaries with various levels of radiation tolerance to use remotely operated processing are not available in the open literature.

Debate over whether subnational groups could plausibly recover plutonium by reprocessing spent fuel from power reactors (which is far more intensely radioactive than typical spent fuel from research reactors) has been ongoing for decades.[227] There appears to

---

[227] An early contribution to this debate was an Oak Ridge memorandum that offered a design for a "simple, quick" reprocessing plant that the authors argued could be built and operated covertly in a short time for low cost. See D.E. Ferguson, "Simple, Quick Reprocessing Plant" (Oak Ridge, Tenn.: Oak Ridge National Laboratory, 30 August 1977). The implications of this assertion were sufficiently far-reaching that Congress requested the General Accounting Office (GAO) to review the subject. GAO concluded that Oak Ridge had likely understated the difficulty of building and operating such a plant. See U.S. Congress, General Accounting Office, *Quick and Secret Construction of Plutonium Reprocessing Plants: A Way to Nuclear Weapons Proliferation?* EMD-78-104 (Washington, D.C.: GAO, 1978). Much, though not all, of that debate was focused on what states could do covertly, rather than on what subnational groups could do. More recently, the Proliferation Vulnerability Red Team, while arguing that a radiation barrier requiring remote operations is a major barrier to recovery, requiring more time, more people, more complexity, and the like, nevertheless took the view that reprocessing of spent power reactor fuel by a subnational group is quite plausible. Hinton et al., *Proliferation Vulnerability Red Team Report*, pp. 4.4-4.6. The team did not, however, explicitly examine the increased risk, with remote operation, of mistakes and problems that could end or greatly delay the effort. Moreover, the team's conclusion should be considered in the light of their assertions regarding the scale of the subnational groups they envision: "access to billions of dollars to fund the acquisition of weapons material using increasingly sophisticated sources and methods" was considered "within the purview of many credible threats." Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 2.1. This debate over the feasibility of small, simple reprocessing plants is reviewed in detail, primarily in the context of covert reprocessing by states (rather than terrorist reprocessing), in Victor Gilinsky, Marvin Miller, and Harmon Hubbard, *A Fresh Examination of the Proliferation Dangers of Light Water Reactors* (Washington, D.C.: Nonproliferation Policy Education Center, 2004). The NAS panel on the spent fuel standard did not dwell at length on this topic, remarking only that "the need for shielding against this [radiation] field complicates the technical work [of chemical separation]...and it poses a risk of health-damaging or even fatal doses of radiation to the operators in the event of mistakes or in the event of a need for "hands on" repairs during processing." U.S. National Academy of Sciences, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options*, p. 52. Since all the disposition forms they examined had substantial radiation fields requiring remote processing, they did not consider what level of radiation field might be required to force the adversaries to shift toward remote processing of the material.

be general agreement that radiation levels sufficient to require remote processing – probably in the range of several hundred to several thousand rem/hr, depending on the doses the processors were willing to sustain – would pose a very substantial barrier to subnational groups, though possibly not an insuperable one to particularly high-capability groups, especially if they had managed to recruit experts with reprocessing experience.[228]

Summary of Radiological Barriers

Against determined, potentially suicidal terrorists, radiation levels would have to be thousands of rem per hour to offer substantial protection against theft. Lower radiation levels, however, would noticeably increase post-theft detectability and could complicate processing. Overall, radiation levels of a few tens to a few hundred rem/hr would probably only reduce the probability of successful theft and bomb-making by about 20%, compared to unirradiated HEU metal (hence a discount factor of 0.8); radiation levels sufficient to force the use of remotely operated chemical equipment, in the case of materials also requiring complex chemical separations, probably rate a discount factor of 0.1-0.2 (that is, a probability of successful theft and bomb-making some 80-90% less than that of unirradiated HEU metal); and material with radiation levels of 10,000 rem/hr or more at one meter should be considered self-protecting against theft.

DOE's current rules, under which any material emitting 15 rem/hr or more at 1 meter is automatically excluded from the Category I category requiring high levels of protection, are totally unjustified and should be changed.[229] Similarly, the DOE, NRC, and international guidelines that treat nuclear material emitting 100 rem/hr at 1 meter or more as self-protecting against theft are indefensible in an age of suicidal terrorists and should be revised.[230]

---

[228] For one official discussion, see U.S. Department of Energy, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*, pp. 53-57.

[229] DOE's graded safeguards table appears in its order on material accounting; at this writing, the most recent version is U.S. Department of Energy, *Nuclear Material Control and Accountability*, DOE M 470.4-6 (Washington, D.C.: DOE, 2005). That table refers to "moderately irradiated" material without defining the term; while the new directive no longer refers explicitly to the 1995 implementation manual, the rules in that manual, which specify that moderately irradiated means 15 rem/hr, are still in use at the sites until the ongoing development of new categorization approaches is completed. (Interviews with DOE officials, July 2006.) See U.S. Department of Energy, *Guide to Implementation of DOE 5633.3b*.

[230] The physical protection convention and IAEA recommendations indicate that if material meets the 100 rem/hr at 1 meter standard, material that would otherwise be considered Category I can be treated as Category II, and Category II material can be reduced to Category III. See International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*; International Atomic Energy Agency, *The Convention on Physical Protection of Nuclear Material*, INFCIRC/274/Rev. 1 (Vienna: IAEA, 1980; available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml as of 29 July 2005). DOE and NRC go further, however. In DOE's system, material that meets the 100 rem/hr at 1 meter standard is automatically Category IV, requiring virtually no physical protection at all, even if it is otherwise pure weapon-grade HEU or plutonium. See U.S. Department of Energy, *Guide to Implementation of DOE 5633.3b*. In the NRC system, material emitting more than 100 rem/hr at 1 meter is exempt from the requirement that it be protected against the design-basis threat for theft; is exempt from most security requirements during transport; and does not require on-site armed guards, or guarded perimeters, or any of the other specific elements of physical protection systems for fixed sites. See U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials."

The Case of Fresh or Irradiated Research Reactor Fuel

In considering what types of security measures should be required at HEU-fueled research reactors, it is useful to envision the series of steps that adversaries would have to take to steal such fuel and make a bomb from it and how the properties of both the research reactor itself and the HEU fuel from it interact to affect the probability that the adversaries would be successful at each step on that path.

To accomplish this mission, outsider adversaries would first have to gain access to the research reactor area (which might require breaking a lock, overcoming a guard, having one or more insider accomplices, or other measures). Then they would have to get access to either fresh fuel that existed on-site, fuel in the reactor core itself (which might take some time to get to, as discussed below), or irradiated fuel that might be stored in a pool. The next step would be to remove fuel elements containing the desired amount of HEU and carry them out to a vehicle; research reactor fuel elements are typically small and light enough to carry relatively easily (or a dolly or similar piece of equipment could be used), but in many cases these fuel elements might only have 50-300 grams of HEU per element, so a large number of elements would have to be stolen.[231] Because this might take some time, they would probably have to either defeat the alarm system at the site or be prepared to fight off the response at least from local or university police, who might arrive relatively quickly. (More substantial response forces would typically take longer to arrive.) Then they would have to drive the material away and elude whatever pursuit and search might follow the theft. After that, they would be faced with the task of chemically processing the material to recover the HEU and then fashioning that HEU into a workable bomb. Finally, they would have to deliver and detonate their bomb. Insider thieves would have to take much the same set of steps, but would have an easier time doing so, as they would already have authorized access to the facility and possibly to the material, would have knowledge and training in matters such as how to remove and handle the fuel, and might have knowledge of the specifics of the security system and its weaknesses as well. The difficulties at each of these steps are real, though not overwhelming – and vary substantially depending on the specifics of the individual research reactor and the type of material it uses.

First, one has to consider how the arrangement of the reactor itself – the facility "environment" – would affect the difficulty of carrying off a successful theft of HEU. This varies depending on whether the fuel in question has not yet been loaded into the reactor; is physically in the reactor; or is in the storage area for irradiated fuel (typically a pool). It also varies depending on the reactor design.

Many research reactors around the world arrange their fuel management to minimize the amount of fresh HEU present: in these cases, fresh fuel is loaded into the reactor shortly

---

[231] As one typical example, a 19-plate Materials Test Reactor (MTR) fuel element has a total weight of just over 6 kilograms; while the uranium content varies, a "generic" figure in the literature is 236 grams of 93% enriched HEU. See Trent Andes, "Sample Appendix a for Generic MTR Assembly," in *IAEA/USA Interregional Training Course: Technical and Administrative Preparations Required for Shipment of Research Reactor Spent Fuel to Its Country of Origin, 13-24 January 1997, Argonne, Ill.* (Argonne, Ill.: Argonne National Laboratory, 1997; available at http://www.rertr.anl.gov/IAEA197/sampl31a.html as of 20 September 2006).

after it is delivered (unless some unexpected delay arises), and each fuel loading is a small enough amount that they rarely, if ever, have a Category I quantity of unirradiated HEU on-site. In the core of the reactor itself, some reactors might have less than a kilogram of HEU, others might have as much as 10-20 kilograms; in general, only critical assemblies, pulse reactors, and perhaps a few other special cases would be likely to have enough in-core material for a gun-type bomb. Some research reactors have one set of fuel for their entire lifetime and hence have little or no irradiated fuel on-site outside of the reactor core. But research reactors that generate substantial thermal power generally have to discharge irradiated fuel regularly and, unless they have a very good arrangement for transporting irradiated fuel elsewhere for processing, storage, or disposal, often build up substantial quantities of irradiated fuel in a pool or other storage arrangement on-site. Indeed, tons of HEU have built up in irradiated research reactor fuel all over the world, and some research reactor spent fuel is posing significant management problems.[232] Thus, at many research reactors, the bulk of the HEU on-site is in irradiated fuel.

These three categories of material – fresh fuel, in-core fuel, and irradiated fuel – should be considered separately:

- **Fresh fuel.** Fresh HEU fuel might be stored in some type of cask and would typically be in a locked room, cabinet, or vault. Once adversaries got to it, however, it would be relatively straightforward to remove it and carry it to a waiting vehicle.
- **In-core fuel.** For in-core fuel, the difficulty of getting at it and removing it would be significantly greater in many cases. Some research reactors (such as tank-type reactors) have enclosed cores. Heavy blocks of shielding might have to be removed to get access to the core; a top plug might also have to be removed, which might be difficult for adversaries with modest experience and would often require a crane.[233] In such cases, the time required to get access to the core might be substantial, increasing the time available for appropriate response forces to arrive and stop the theft – if the adversaries had not succeeded in defeating the alarm system at the site so that they were not detected. Even once the core had been accessed, some type of tool would be needed to pull the individual fuel elements out; pulling out enough fuel elements to get the HEU for a bomb could take an hour or more.[234] In the case of pool-type reactors, by contrast, the top of the pool can usually be accessed easily, but a tool to pull fuel elements out would still be needed and there would still be the time required to pull the fuel elements out. One Los Alamos analysis prepared for the NRC estimated that removing the fuel elements from the core might take 2 minutes or more per element – meaning an hour or more if 30 fuel elements

[232] Iain G. Ritchie, "Growing Dimensions: Spent Fuel Management at Research Reactors," *IAEA Bulletin* 40, no. 1 (March 1998; available at http://www.iaea.org/Publications/Magazines/Bulletin/Bull401/article7.html as of 20 September 2006). While this paper is now almost a decade old, the situation has improved very little since it was written; far more spent fuel has been generated than has been dealt with in the intervening time.

[233] Moreover, the equipment used for this purpose in normal operation could potentially be locked in a way that would make it very difficult for adversaries to use it. See, for example, discussion in Koelling and Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II.*

[234] Koelling and Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II.*

were needed to get the desired amount of nuclear material.[235] Moreover, for high-power research reactors, fuel pulled right out of the core would be quite radioactive (though this would be less true for lower-power facilities where the short-lived fission products would tend to decay away as fast as they built up); indeed, for many lower-power reactors, it is difficult to keep even the in-core material above 100 rad/hr at 1 meter.[236] To put these difficulties in context, however, it should be remembered that these reactors are designed to allow refueling and other tasks requiring access to the core to be done regularly; these tasks are typically done by students at the universities where many research reactors exist; and all the equipment necessary to gain access to the core and to remove material from the core is available on-site, because it is needed on-site.[237]

- **Irradiated fuel.** As already noted, delays in shipping irradiated fuel away for processing or disposal have led to many sites having large quantities of HEU in irradiated fuel on-site. This material is often stored in pools, where again some type of tool could be used to raise the fuel elements out of the pool one at a time, after which they could be carried to a waiting vehicle, such as a truck.

Critical assemblies and pulse reactors pose important exceptions to the discussion above. Critical assemblies generate virtually no fission products; their fuel, even the in-core fuel, can be considered essentially identical to fresh fuel. In many cases, for convenience of experimenting, the fuel is designed so that it can readily be added to or taken out of the assembly core. (In some cases the researchers do this with their bare hands, the fuel is so non-radioactive.) In the case of pulse reactors, very high power may be generated, but only for a fraction of a second, so again, the buildup of fission products and the resulting radioactivity from the fuel are minimal. Both types of reactors often have far larger quantities of material on-hand than typical research reactors do, in some cases hundreds of kilograms or even tons of material. Moreover, some of these facilities use very highly enriched material, in some cases in metal form. For most critical assemblies and pulse reactors, there would be virtually no facility-related barrier to thieves removing large quantities of HEU – and hence the requirements for security measures at these sites should be higher than for other types of research reactors where more facility-specific barriers are in place.

Research reactor fuel might be stolen from a transport, not just from a research reactor itself. In the United States and a number of other countries, fresh HEU fuel is usually transported in small batches, so more than one transport would have to be seized to get a Category I quantity of nuclear material. Irradiated fuel may be moved in larger quantities, particularly if it is judged to meet the 100 rad/hr at one meter standard for self-protection. During transports, fuel would typically be in large casks, which thieves would have to open in order to gain access to the fuel itself, but for well-prepared thieves with either explosives or

---

[235] Koelling and Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II*, pp. 7-8.
[236] See, for example, discussions in Koelling and Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II*, pp. 7-8; *Conversion of Research and Test Reactors*, pp. 450-452.
[237] For a discussion emphasizing the potential ease of removal of material from reactor cores, see, for example, Daniel Hirsch, "Weapon-Grade Uranium on Campus," reproduced in *Conversion of Research and Test Reactors*, pp. 425-454.

appropriate cutting tools, this should not be unduly difficult; the casks, after all, are designed to be opened after the transport is completed.

In addition to the ease or difficulty of removing the HEU from a research reactor, there is the question of the quality of the material that might be removed. Only a few of the world's research reactors (again, typically critical assemblies or pulse reactors) use large quantities of weapon-grade HEU metal as their fuel. Instead, most HEU-fueled research reactors use fuel that consists of a mix of uranium and aluminum oxides, with aluminum cladding, or a uranium-zirconium-erbium mix (the fuel used by the common "TRIGA" reactors – an acronym for Training, Research, Isotopes, General Atomics). These materials could not be used directly in nuclear explosives; rather, the recipients of such research reactor fuels would have to chemically process them to separate the uranium. (Indeed, many of these fuels contain less than 10% by weight U-235 and hence in DOE's system would always be considered no more than Category II, no matter how many kilograms of HEU was present at a site.)[238]

Aluminum and uranium are chemically quite dissimilar, and the aluminum-uranium separation is one of the easier separations in nuclear chemistry. Typical TRIGA fuel or material test reactor (MTR) plates might be modestly more difficult to cut into pieces than pins from a typical light-water reactor assembly, but this cutting would not be especially difficult. Once in pieces, the fuel can readily be dissolved in hot nitric acid available in quantity from any chemical supply company, and once in solution a wide variety of options are available to separate the uranium, ranging from standard (but somewhat complex) approaches such as solvent extraction to simple approaches such as adding particular chemicals that will cause the uranium to precipitate as a sludge, which can then be recovered and converted to metal with a further round of processing. The facilities for doing this do not have to be complex: for the dissolution and separation, a series of 55-gallon drums will do. James C. Warf, one of the leaders of the chemical processing programs in the Manhattan Project, has argued that "[t]hese are not difficult procedures, particularly for someone intent on acquiring an atomic explosive; one might say, in fact, that they are not beyond the ability of most students in introductory chemistry classes at the college level."[239] Nevertheless, as discussed above, the need for such chemical processing means another set of capabilities that the terrorist group must acquire, more time and equipment needed to get the material for a bomb, and more chances for serious mistakes or for detection of the conspiracy underway.

HEU research reactor fuel also comes in a range of enrichments. Some HEU-fueled reactors, particularly U.S.-supplied facilities or facilities within Russia, continue to use HEU enriched to 90% or more. The HEU-fueled reactors the Soviet Union exported typically used 80% enriched fuel, little different from 90% enriched material in the probability that recipients would be able to make it into a bomb. But during the 1980s, most of these reactors were converted to use 36% enriched fuel, which is much less attractive for weapons use, as

---

[238] See, for example, the fuel element weights and the weights of contained uranium for generic MTR (materials test reactor) fuel elements, provided in Andes, "Sample Appendix a for Generic MTR Assembly."
[239] James C. Warf, statement in *Conversion of Research and Test Reactors*, pp. 514-516.

discussed above. (Efforts are now underway to convert both the U.S.-supplied and Soviet-supplied HEU-fueled reactors to use LEU fuel.)

The HEU fuel that might be stolen could be fresh fuel, in-core fuel, or irradiated fuel. Fresh fuel would not have any significant radiation barrier to theft or processing, but in-core or irradiated fuel would. The characteristics of irradiated HEU fuel vary, of course, depending on the specifics of the reactor and the irradiation history of the fuel. The two most important differences between fresh HEU fuel and irradiated HEU fuel are the enrichment of the material and the radiation level of the material.

HEU research reactor fuel is often irradiated to burnups of 40-60% of the fissile atoms. A burnup of 50% does not, however, cut the enrichment in half. Fuel that was 90% enriched initially and is irradiated to a burnup of 50% will still be over 80% enriched when discharged.[240] Hence, with respect to enrichment level, HEU fuel that initially had very high enrichments ends up only modestly less attractive for weapons use after irradiation.

The other major difference between fresh and irradiated fuel is the radiation level of the irradiated fuel. But irradiated research reactor fuel is very different from spent fuel from power reactors. Unlike the massive, intensely radioactive fuel assemblies from a light-water reactor (LWR) operated to a typical burnup, typical research reactor fuel assemblies are physically small and light enough for one person to carry, or even to put in a backpack, and the radiation fields they emit are far lower. Typical Materials Test Reactor (MTR) fuel elements with 300 grams of 93% enriched uranium per element, burned to 50% of fissile atoms, will no longer meet the 100 rem/hr at one meter standard 10-12 years after discharge (depending on the power generated per kilogram of U-235 during irradiation).[241] IRT fuel elements used in many Soviet-designed reactors behave in a roughly similar way, but fuel elements from the common TRIGA reactors will typically cool to below 100 rem/hr at one meter in a couple of years after discharge.[242] The IAEA experts who manage a database on irradiated research reactor fuel around the world believe that most of the world's irradiated research reactor fuel does not meet the 100 rem/hr standard.[243]

As noted earlier, fuel delivering a radiation dose in the range of 100 rem/hr at one meter would not pose any substantial obstacle to theft by individuals who did not care about their own health or safety. The vehicle carrying the stolen fuel away from the theft site would be easier to detect than would be the case for fresh fuel, if responders were able to get

---

[240] As a simplification, if 9 out of every 10 of the original uranium atoms were U-235, and half of those 9 atoms have been destroyed, then 4.5 of the remaining 5.5 uranium atoms (81%) are U-235. To get a more precise accounting taking into account the fact that a small portion of the U-238 is also destroyed requires more detailed modeling.

[241] See R.B. Pond and J.E. Matos, *Nuclear Mass Inventory, Photon Dose Rate, and Thermal Decay Heat of Spent Research Reactor Fuel Assemblies (Rev. 1)*, ANL/RERTR/TM-26 (Argonne, Ill.: Argonne National Laboratory, 1996).

[242] Calculations by Bryan Broadhead, Oak Ridge National Laboratory. Personal communication, October 2006. Broadhead's calculation related to IRT fuel was specifically for the 36% enriched type still in wide use. Few, if any, reactors outside Russia still use the previous 80%-enriched fuel, and for the reactors outside Russia, that fuel will in general have been cooling long enough that it no longer emits 100 rem/hr at 1 meter.

[243] Interview with Iain Ritchie, IAEA, September 2002.

helicopters or airplanes with effective radiation detectors searching very soon after the theft – but as discussed above, the increase in the probability of catching the perpetrators from this additional radiation is likely to be quite modest. The chemical processes that would have to be used to separate the uranium from the rest of the material would be identical to those required for fresh fuel, and if those conducting these processes also did not care about their health and safety, remote operations would not be required.

Overall, then, the HEU in fresh research reactor fuel would pose a substantial risk if stolen; a discount factor in the range of 0.6, compared to the risk posed by HEU metal of equivalent enrichment, seems appropriate – toward the high end of the range for materials requiring chemical processing, discussed above. For irradiated research reactor fuel with radiation levels in the range of 100 rem/hr at one meter or lower, a discount factor in the range of 0.4, compared to HEU metal of equivalent enrichment, seems appropriate (that is, this radiation level might reduce the chance that recipients could make a bomb from the stolen material by a further one-third compared to unirradiated research reactor fuel at the same enrichment).

The Case of Unirradiated Plutonium-Uranium Mixed Oxide (MOX) Fuel

Another type of material that is in common civilian use and whose security risks are often debated is unirradiated MOX power reactor fuel. Currently, because fast-neutron reactors have not yet been commercialized, MOX fuels are predominantly used in light-water reactors. MOX fuel assemblies for such reactors are large and heavy. The total weight of a pressurized water reactor (PWR) fuel assembly (the most common type of reactor using MOX) is 658 kilograms; they are about 4 meters long.[244] 461 kilograms of this total weight is heavy metal (uranium or plutonium) in the fuel, of which approximately 7% by weight, or roughly 32 kilograms, might be plutonium in a typical MOX assembly. Hence adversaries considering a theft from a facility where such assemblies were located would have to choose whether to carry off an entire MOX assembly or whether to try to separate a part of the assembly (possibly with explosives). In most cases, the measures needed to carry off only, say, one-third of the assembly would be likely to be more trouble than carrying off the entire assembly. At a typical reactor site, MOX assemblies before loading might be stored in a locked area near the reactor, or they might be stored in the spent fuel pool pending insertion in the reactor. In either case, the thieves would have to overcome whatever security was provided for the facility; in the case of MOX assemblies stored in the spent fuel pool, they would also have to (a) determine which assemblies were the unirradiated ones (possibly on the basis of the Cerenkov glow, which is routinely used by IAEA inspectors to confirm that the assemblies in a pool are irradiated fuel) and (b) lift the assembly out of the pool, a task which would require special equipment. While fuel-lifting equipment would be available on-site, it might be locked in a way that would make it difficult for adversaries to use. Once they had gotten an assembly, the adversaries would have to get it out to a vehicle and drive it away, coping with whatever response, pursuit, or search ensued. Given the size and weight of

[244] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 270. Boiling-water reactor (BWR) assemblies are about one-half as heavy, with a similar length.

the assembly, even a very minimal security system should make it possible to ensure that such a removal would be detected, so that the theft would have to be overt; on the other hand, any thieves remotely capable of taking on the security at a typical reactor site should have little difficulty carrying the assembly to a vehicle and providing a vehicle large enough to transport it. Of course, as with research reactor fuel, the thieves might steal the material from a transport or a fuel fabrication site, rather than a reactor site.

Once adversaries had a MOX assembly, they would have to chemically process it to recover the plutonium. This would require cutting the fuel rods into pieces, dissolving them in hot acid, and then separating the plutonium from the solution, for example by solvent extraction or by ion exchange. The uranium-plutonium separation is somewhat more difficult than the uranium-aluminum separation, but it has been performed in many facilities in many countries, and the procedures for the separation have been published in detail. The recovered plutonium would then have to be reduced to metal (unless the adversaries were planning to use the recovered form directly in a bomb, which might be possible in some cases). As discussed above, all of the required equipment and chemicals are commercially available and could be purchased without raising undue attention. On the other hand, having a MOX assembly rather than plutonium or HEU metal would mean that the recipients would have to: recruit people with knowledge of chemical processing; prepare facilities, equipment and materials for that purpose; allow more time to prepare for bomb manufacture; face a larger number of chances to make serious mistakes or for the operation to be detected. The Proliferation Vulnerability Red Team, for example, estimated that to get plutonium metal from MOX, some nine chemical processing steps would be needed; three months would likely be required to prepare the necessary facilities and equipment; and six weeks would then be needed to do the processing.[245]

There has been a long-standing debate over the years over how much protection was afforded by plutonium being in the form of unirradiated MOX fuel assemblies. Many in the plutonium recycling industry have argued that fabricated MOX fuel elements pose little threat of theft, because of the difficulties of stealing such large, heavy objects and the difficulties of processing them to recover plutonium. Japan, for example, has adopted a policy of having plutonium recovered from reprocessing in Europe shipped to Japan in the form of fabricated MOX fuel elements, in part to limit controversies over the risks of theft during these long and readily tracked sea shipments. Others – especially those opposed to plutonium recycling and to the use of MOX for disposition of excess weapons plutonium – have long argued that the theft risk posed by plutonium in MOX fuel is only modestly less than the risk posed by other plutonium. The U.S. government has insisted, in international discussions, that MOX must be considered Category I material like other plutonium. A detailed review of proliferation risks by a committee of the National Academy of Sciences recommended that MOX fuel be subject to security standards comparable to those applied to intact nuclear weapons (which the panel called the "stored weapon standard"). Such standards should be applied: [246]

---

[245] Hinton et al., *Proliferation Vulnerability Red Team Report*, p. 4.4.

[246] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 72.

> up to the point in the [plutonium] disposition process where the spent fuel standard has been attained. The argument for the stored weapons standard is that the pathway leading from any separated plutonium form (a pit, an ingot, plutonium oxide, or even plutonium and uranium mixed oxide) is sufficiently direct and easily traversed by at least some potential proliferators that applying *less* than the stored weapons standard to the protection of such material could lead to the highly undesirable result that dismantlement of surplus nuclear weapons and disposition of their nuclear-explosive materials could produce an *increase* in proliferation risk.

Overall, this panel, assigning numerical ratings from 0-4 for the overall barriers to recovery of plutonium from different forms for use in weapons (where 0 is insignificant and 4 is a very large barrier), rated MOX powder at "2-", MOX fuel rods at "2" and MOX assemblies as "2+". In other words, the additional benefit of the large size and mass of the assemblies was considered to be real but quite modest, while the barrier posed by the need to chemically process the MOX to recover the plutonium was considered to be quite significant, though not insuperable.[247] Similarly, the laboratory team referred to earlier rated the difficulty of recovering plutonium for weapons from MOX fuel as "medium" (with the difficulty of reducing pure oxide to metal "low," and the difficulty of recovering plutonium from spent fuel "high").[248] The Proliferation Vulnerability Red Team argued that the large size and mass of MOX assemblies would make covert theft "non-credible," but would not be a major barrier to overt theft and that while the chemical processing required was significantly more complex than for pure plutonium oxides, it would not be unduly difficult for adversaries to accomplish.[249] In a detailed government study on MOX security from the 1970s, the NRC staff categorized unirradiated MOX fuel as requiring "relatively modest facilities and effort" to recover the plutonium for use in a bomb.[250] That study concluded that since separating plutonium from MOX "could be within the capabilities of some malefactors... lowering the concentration of plutonium through blending should not be used as a basis for reducing the level of safeguards protection," though it would increase the mass of material adversaries would have to steal to get enough for a bomb and increase the time required between the theft and having a usable nuclear explosive.[251]

More recently, the NRC has taken a starkly different view in an extended (though largely classified) debate concerning how attractive MOX fuel might be to potential thieves in the context of licensing U.S. reactors to use MOX fuel for the U.S. weapons plutonium disposition program. Duke Power asked for an exemption from many of the specific physical protection requirements for Category I facilities, based on the specific characteristics of the material in MOX fuel assemblies and the level of security that power reactors have been required to have since 9/11 to protect against sabotage. Critics tried to block these exemptions, arguing that potential adversaries might well be able to steal and process

---

[247] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, p. 275.
[248] "Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," p. 12.
[249] Hinton et al., *Proliferation Vulnerability Red Team Report*, pp. 4.6, 4.8, 4.13-14.14.
[250] Office of Nuclear Material Safety and Safeguards, *Safeguarding a Domestic MOX Industry*, p. 3.16.
[251] Office of Nuclear Material Safety and Safeguards, *Safeguarding a Domestic MOX Industry*, pp. 6.8-6.9.

plutonium in MOX fuel, while Duke and the NRC staff argued that MOX fuel assemblies would be highly unattractive targets for theft. The Atomic Energy Licensing Board concluded that theft of fresh MOX fuel represented a real risk; the NRC disagreed, arguing that MOX fuel would not be an attractive target for potential thieves.[252] Unfortunately, all of the specifics of these arguments are considered confidential safeguards information and have not been released.[253] It does not appear, however, that NRC had any new information available to it that demonstrated that recovering plutonium from MOX was more difficult than the NRC staff concluded it was three decades ago; rather, the current Commissioners appear to have drawn different judgments from a similar underlying set of facts.

Remarkably, at one point in the proceedings, the NRC argued that there was "no rational reason" why a reactor with unirradiated MOX fuel assemblies should have any greater security than other reactors.[254] Not surprisingly, given that view, the NRC ultimately granted the exemptions Duke requested. Though Duke did not ask for and was not granted an exemption from the fundamental requirement to be able to defend against the NRC's DBT for theft, it was permitted to defend only against the pre-9/11 DBT; NRC explicitly ruled that while it had ordered the two large HEU-processing facilities it regulates to put in place measures to defend against a larger design basis threat after the 9/11 attacks, those orders applied only to those facilities, and reactors with MOX fuel would not be required to meet those post-9/11 requirements.[255]

In thinking through what position to take in this debate, it is important to remember that making an implosion-type bomb from pure plutonium would already require a highly sophisticated terrorist group with substantial capabilities; while stealing and processing MOX assemblies would clearly require more capabilities and involve more opportunities for mistakes or detection, it seems likely that the point the National Academy panel made about extracting plutonium from a glass log with no fission products in it would also apply to a MOX fuel assembly with no fission products in it: "most potential proliferators with the technical expertise, personnel, and the organization required to produce an operable weapon from separated plutonium – a substantial task in itself – would also be able to extract plutonium chemically" from such an assembly.[256]

Ultimately, as plutonium metal already has a discount factor of 0.6 compared to HEU metal, a further discount factor of an additional 0.6 for MOX fuel assemblies (compared to plutonium metal) appears appropriate.

---

[252] U.S. Nuclear Regulatory Commission, *In the Matter of Duke Energy Corporation (Catawba Nuclear Station, Units 1 and 2)*, CLI-05-14 (Washington, D.C.: NRC, 2005; available at http://www.nrc.gov/reading-rm/doc-collections/commission/orders/2005/2005-14cli.html as of 22 Sepember 2006).

[253] References to relevant page numbers from the confidential proceedings are cited in U.S. Nuclear Regulatory Commission, *CLI-05-14*.

[254] U.S. Nuclear Regulatory Commission, *CLI-04-29*.

[255] U.S. Nuclear Regulatory Commission, *CLI-04-29*. Remarkably, the NRC also overruled the Atomic Energy Licensing Board's decision to require Duke to prove, in a realistic test, that it *could* defend against the pre-9/11 DBT – even though Duke had not objected to that requirement. See U.S. Nuclear Regulatory Commission, *CLI-05-14*.

[256] U.S. National Academy of Sciences, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options*, pp. 225-226.

Risks Posed by Different Types of Nuclear Weapons

Clearly, theft of any type of assembled nuclear weapon would pose an immense threat. Every assembled nuclear weapon deserves the highest practicable levels of protection. But it is worth briefly considering how the risks posed by successful nuclear theft vary with the particular type of weapon stolen, and how the risks posed by theft of an assembled weapon might compare with the risks posed by theft of weapons-usable nuclear material. Several factors affect the probability that terrorist recipients would be able to make use of a stolen nuclear weapon.

Weapon Technical Safeguards

If terrorists could figure out how to detonate it, an assembled nuclear weapon would have the immense advantage of being already assembled and ready to go. Moreover, in most cases, assembled weapons would have much larger explosive yields than terrorists are likely to achieve with a crude bomb of their own: most public estimates of plausible yields for a terrorist nuclear bomb are in the 1-20 kiloton range, while most nuclear weapons in the arsenals of states have yield in the range of 100-500 kilotons.

But detonating a stolen nuclear weapon may be a substantial challenge for a terrorist group that receives it. Even a weapon with no built-in technical safeguards may pose a difficult puzzle as to how it should be set off, if the recipients do not also get any insider information about the weapon. But as discussed in Chapter 2, many modern weapons are equipped with features that make them quite difficult to detonate, some designed for security and some for safety.

Overcoming an electronic or electromechanical lock designed to prevent the weapon from being armed and detonated unless the correct code is inserted (known in the United States as a Permissive Action Link, or PAL) would be a substantial challenge, particularly if the PAL were a modern design, made to be very difficult to bypass and "hotwire" the warhead and equipped with "limited try" features designed to permanently disable the weapon if too many wrong codes are inserted.[257] Unfortunately, older Russian tactical nuclear weapons reportedly are not equipped with PALs, or are equipped with older designs that may be easier to bypass.[258] How many of these weapons still exist is not publicly known. Similarly, since U.S. PALs were introduced to address perceived risks posed by forward-deployed tactical

---

[257] For discussions of PALs, see Donald R. Cotter, "Peacetime Operations: Safety and Security," in *Managing Nuclear Operations*, ed. Ashton B. Carter, Charles A. Zraket, and John D. Steinbruner (Washington, D.C.: Brookings Institution, 1987); Peter Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, N.Y.: Cornell University Press, 1992); Peter Stein and Peter Feaver, *Assuring Control of Nuclear Weapons: The Evolution of Permissive Action Links*, Csia Occasional Paper, No. 2 (Cambridge, Mass.: Center for Science and International Affairs, Harvard University, 1987).

[258] For a press report ostensibly describing U.S. intelligence estimates on this subject, see Bruce W. Nelan, "Present Danger: Russia's Nuclear Forces Are Sliding into Disrepair and Even Moscow Is Worried About What Might Happen," *Time Europe* 149, no. 14 (7 April 1997), p. 42. See also the testimony of Bruce G. Blair in National Security Committee, Military Research & Development Subcommittee, *Hearing on Russian Missile Detargeting and Nuclear Doctrine and Its Relation to National Missile Defense*, U.S. House of Representatives, 105th Congress, 1st Session, 13 March 1997 (available at http://armedservices.house.gov/testimony/105thcongress/97-3-13Blair.htm as of 28 February 2006).

nuclear weapons, in the U.S. stockpile PALs were not applied to strategic ballistic missile warheads.[259]

Environmental sensing devices (ESDs), designed to prevent a weapon from arming and detonating until it has gone through the expected flight-to-target sequence (such as several minutes of boost phase acceleration followed by free flight, in the case of a ballistic missile) were designed for safety, not security, but are also likely to complicate the recipients' efforts to set off a stolen bomb significantly.[260] Weapons incorporating modern PALs and ESDs pose a significantly lower probability that terrorists would succeed in detonating them than weapons without these features.

Some less developed nuclear states, such as Pakistan, are not believed to incorporate advanced technical safeguards into their weapon designs. But in Pakistan, weapons are believed to be stored in disassembled form, perhaps with key nuclear components needed for the weapon to detonate in two separate locations;[261] such an approach may be as effective as PALs in reducing the dangers posed by nuclear theft.

Quantities of Nuclear Material Contained in a Weapon

Even if the recipients of a stolen nuclear weapon could not find a way to set it off, they could cut it open and try to use the nuclear material inside to make a crude bomb of their own. This nuclear material would typically be plutonium or HEU metal, or both. The terrorists might try to put their own explosives around the metal ball of weapons-usable nuclear material known as the primary, or "pit," without changing its configuration at all. For some weapons, this might work (and thereby reduce the number of tasks the terrorists would have to accomplish significantly, compared to manufacturing a pit of their own); in the case of a highly efficient modern pit design, however, the weapon might contain so little nuclear material in the primary that it could be difficult to get a substantial yield from it with a crude terrorist arrangement of explosives.

But modern thermonuclear weapons will also have a "secondary" component, which contains HEU. The HEU in the secondary alone might be sufficient, when cast and machined to appropriate shapes, for a crude implosion bomb.[262] If not, the combination of the primary material and the secondary material should be more than enough to make a crude implosion bomb – though if the primary was made from plutonium (as most are) and the secondary from HEU, this would require the recipients to master working with both metals. Few assembled weapons that are not themselves gun-type bombs are likely to contain enough HEU for a gun-

---

[259] For a discussion of which U.S. warheads have which types of PALs, see Cochran, Arkin, and Hoenig, *Nuclear Weapons Databook: Volume I.*

[260] For a discussion of ESDs, see Cotter, "Peacetime Operations: Safety and Security."

[261] See, for example, Lee Feinstein et al., *A New Equation: U.S. Policy toward India and Pakistan after September 11* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.ceip.org/files/pdf/wp27.pdf as of 4 October 2006), p. 39.

[262] One unclassified estimate suggests that a typical modern thermonuclear warhead contains 15-30 kilograms of HEU. See David Albright, Frans Berkhout, and William B. Walker, *Plutonium and Highly Enriched Uranium, 1996: World Inventories, Capabilities, and Policies* (Solna, Sweden; Oxford, UK; and New York: Stockholm International Peace Research Institute (SIPRI) and Oxford University Press, 1996), p. 90.

type bomb. In general, weapons with large amounts of material in their primary (so that terrorists might be able to get a substantial yield from the primary with their own explosives, without modifying the primary) should be considered to pose a somewhat greater risk than other weapons.

Weapon Size and Mass

While stories of "suitcase bombs" capture the public imagination, a good case can be made that over a broad range that covers most modern nuclear weapons, smaller, lighter weapons would be only slightly easier for thieves to steal. Thieves sophisticated enough to have any chance at all of success in stealing a nuclear weapon will surely bring a vehicle suitable for transporting the stolen weapon or weapons from the site and will surely have several people involved in the theft. So as long as a weapon is small enough that it can be lifted to a nearby vehicle by several people – perhaps using a dolly or similar simple equipment – and can be carried by a common-place vehicle, it is likely to be almost as easy to steal as a smaller weapon would be. The most massive bombs ever built in the United States and the Soviet Union, weighing many tons each, would indeed pose a significant size and mass barrier to theft; but as discussed above in the section on size and mass of material that has to be stolen, typical modern weapons, many of which are designed to be carried by long-range missiles (putting a premium on weight) have weights in the range of a few hundred kilograms or less. Anyone who could accomplish the very difficult job of arranging a theft of a nuclear weapon would have a very high probability of succeeding in the far simpler job of arranging for transport of such a weapon.

Tactical vs. Strategic Weapons

Many analysts argue that tactical nuclear weapons pose a higher risk of nuclear theft than do strategic nuclear weapons, because (a) tactical weapons are less likely to be equipped with effective technical safeguards against unauthorized use; (b) tactical weapons are smaller and easier to steal; and (c) tactical weapons are more likely to be located at forward-deployed and less secure storage facilities.[263]

As noted above, published reports suggest that it is correct that Russian tactical weapons are less likely to have effective PALs, but the opposite is true for U.S. nuclear weapons. The argument that tactical weapons are smaller and lighter is certainly true for some tactical weapons (such as nuclear artillery shells or atomic demolition munitions, for example), but in other cases the sizes are similar; indeed, some weapons in both the United States and Russia (such as the B61 bomb) are slated for both tactical and strategic missions. Many of the smallest tactical weapons (including, apparently, all nuclear artillery shells and all U.S. atomic demolition munitions) have been dismantled, in part as a result of the 1991-1992 Presidential Nuclear Initiatives (PNIs). In any case, as just argued, few remaining strategic weapons are massive enough that their sheer size and mass would pose much of an obstacle to theft. It was overwhelmingly true in the past that tactical weapons were spread at

[263] See, for example, Potter and Sokov, "Practical Measures to Reduce the Risks Presented by Non-Strategic Nuclear Weapons."

forward-deployed and potentially less secure sites: U.S. tactical weapons were deployed all over the world, and Soviet tactical weapons were deployed in most republics of the Soviet Union and in Eastern Europe as well.[264] But the pull-backs before and after the 1991-1992 PNIs have dramatically changed that situation. Today, most U.S. and Russian tactical weapons have been dismantled, and most of the remainder are in central storage facilities. Russian tactical weapons exist only in Russia, largely in centralized national-level storage facilities (though some service-level tactical storage sites still exist);[265] a modest number of U.S. tactical air-delivered bombs are still deployed in Europe, and the remaining U.S. tactical weapons are in centralized storage in the United States. In short, tactical and strategic nuclear weapons both pose risks of nuclear theft; there is no reason to focus greatly more attention on one type of weapon than on the other.

Stolen Weapons vs. Stolen Materials

Theft of either an assembled nuclear weapon or enough plutonium or HEU for a crude nuclear bomb would pose an immense danger. But what can be said about the relative risks posed by each?

I would argue that the various types of items that might be stolen rank roughly as follows (in order of descending probability of the recipients being able to achieve a substantial-yield nuclear explosion from them):

1. Enough high-grade HEU metal for a gun-type bomb
2. An assembled nuclear weapon without technical safeguards
3. An assembled nuclear weapon with effective technical safeguards
4. Enough HEU or plutonium metal for an implosion-type bomb
5. Enough HEU or plutonium for an implosion-type bomb in direct-use or easily convertible compounds and mixes (e.g., oxides, nitrates)
6. Enough HEU or plutonium for an implosion-type bomb in compounds and mixes requiring complicated chemical separations

In this listing, a large quantity of HEU metal comes first because the information needed to achieve a nuclear explosion is in the unclassified literature and the equipment needed is readily commercially available. By contrast, none of the information needed to figure out how to detonate an assembled weapon would be publicly available. An assembled weapon, even with effective technical safeguards, ranks modestly higher than enough HEU or plutonium metal for an implosion-type bomb, as there would be some non-zero chance that

---

[264] William M. Arkin and Richard W. Fieldhouse, *Nuclear Battlefields: Global Links in the Arms Race* (Cambridge, Mass.: Ballinger, 1985).

[265] The best available current accounts of Russian tactical nuclear weapons and the issues they raise are Gunnar Arbman and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part I: Background and Policy Issues*, vol. FOI-R--1057--SE (Stockholm: Swedish Defense Research Agency, 2003); Gunnar Arbman and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part II: Technical Issues and Policy Recommendations*, vol. FOI-R—1588—SE (Stockholm: Swedish Defense Research Agency, 2005; available at http://www.foi.se/upload/pdf/FOI-RussiasTacticalNuclearWeapons.pdf as of 12 April 2005).

the terrorists could figure out how to detonate the weapon, or to use its primary for their bomb without modification, and even if neither of those could be done, in most cases the weapon would still contain enough plutonium or HEU (or both) for an implosion-type bomb.

But several factors suggest that assembled weapons deserve at least as much security as large stocks of HEU metal, even if the weapons are equipped with effective technical safeguards. First, terrorists who had a stolen nuclear weapon would be in a position to make fearsome threats—for no one would know for sure whether they could set it off or not. Second, as noted earlier, if they did succeed in setting off a stolen weapon, the explosive yield of most weapons would be much higher than the likely yield of a crude terrorist bomb. Third, an assembled nuclear weapon, by its nature, contains nuclear weapon design information, which itself should be protected from transfer either to terrorist groups or to states. Hence, like large quantities of HEU metal, I assign assembled nuclear weapons a discount factor of 1.0, meaning that they require the highest levels of protection.

Implications: A New Approach to Categorizing Nuclear Materials

These considerations suggest that significant modifications should be made in DOE's approach to categorizing nuclear materials, the approaches in NRC regulations, and the international approaches included in the IAEA's recommendations.

A completely graded approach might have almost continuous variations in the intensity of security measures with increasing quantity and quality of the nuclear material at a facility or transport leg. It would not be very practical, however, to have regulations that required frequent changes in security arrangements resulting from even modest changes in the nuclear material on-site. Moreover, with the basic Category I, II, and III structure having been in place for decades and enshrined in difficult-to-alter international legal agreements such as the Convention on Physical Protection, it is useful to attempt to stick with that structure as much as possible.

A more graded approach that sticks with that structure is possible, however. In the approach proposed here, regulators would assign discount factors, as discussed above, for material that posed various barriers to successful bomb-making – and would then set security rules that would allow correspondingly higher probabilities of successful theft for material that would offer adversaries less chance of successfully manufacturing a nuclear bomb. Regulators might adjust the probability of successful theft by requiring facilities to be defended against a smaller DBT (which might therefore have a higher probability that adversaries would exceed it and overwhelm the security system at a facility); by requiring facilities to achieve only a lower probability of defeating a fixed DBT; or, in a rule-based approach, by modifying particular security requirements.

The threat spectrum faced by Country A in Table 4.1 at the beginning of this chapter can serve as an example. If regulators in Country A set a DBT corresponding to the middle of that threat spectrum (4-9 well-armed, well-trained outsiders, 1-2 insiders, or both) and required facilities with large quantities of HEU metal to put in place security measures that were judged to have a 95% chance of defeating that threat, these measures' probability of defeating the lesser threats in the table would probably be close to 100%. Even if these

Table 4.9: Proposed Categorization of Nuclear Materials: Quantity

	Pu[a] or U-233	HEU	Disc. Factor
Category I	≥ 2 kg	≥ 5 eff. kg[b]	1.0
Category II	> 500 g < 2 kg	>1 eff. kg < 5 eff. kg	0.3
Category III	> 15 g ≤ 500 g	> 15 eff. g ≤ 1 eff. kg	0.1

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
[b] Effective kilograms=kilograms of uranium times the square of the fractional enrichment.

measures had only a 50% chance of defeating the next higher level of threat and no chance at all of defeating the highest level of threat, their overall probability of effectiveness would be 93% (given the probabilities assigned to the different levels of threat in the table). If regulators considered that sufficient for a large quantity of HEU metal, they might conclude that for fabricated MOX fuel, for example, with a discount factor in the range of 0.4, facilities could be required to have security measures offering lower confidence in defeating the DBT, so that the overall probability of a theft attempt being successful, rather than 7%, would be in the range of 17%. This would leave the overall estimated risk the same as that for the HEU metal, if the probability of any type of theft attempt occurring did not change.

Table 4.9 outlines the first step in this revised approach, focused on the quantity of different types of materials. The thresholds are the same as those in the current IAEA, NRC, and DOE rules – except that for HEU, the quantity is measured in "effective kilograms" of HEU (kilograms of total uranium multiplied by the square of the fractional enrichment), to better reflect the increasing quantity of material required as enrichment is reduced. (As noted earlier, the term effective kilograms, measured in this way, is already used in IAEA safeguards.) In this approach, as noted earlier, 5.8 kilograms of 93% enriched HEU would be a Category I quantity, but it would take 31.2 kilograms of 40% enriched HEU to be a Category I quantity. The specific discount factors proposed here are somewhat arbitrary. I suggest 0.3 for Category II because, while it would take only two thefts of Category II quantities to get to a Category I quantity, it would require roughly four of the largest Category II quantities to reach the rough 7.5-kilogram threshold of enough plutonium for a crude bomb (counting likely process losses) discussed above, or the roughly 22.5-kilogram threshold for HEU. As discussed above, arranging two thefts would be more than twice as difficult and risky as arranging one, and arranging four thefts would be more than four times as difficult as arranging one. The comparison to the Category I threshold suggests that the correct figure should be below 0.5, while the comparison to the amount required for a bomb suggests that the correct figure should be one-quarter or less; 0.3 is this a compromise, with an element of conservatism (similar to the conservatism also reflected in the size of the thresholds for Category I materials). The 1990s DOE consequence ratings cited above assign a 0.4 rating to Category II material, reflecting a modestly greater degree of conservatism. For Category III material, I suggest a 0.1 figure, again roughly one-third that of the next highest level, for similar reasons. The 1990s DOE consequence ratings are again more conservative, giving Category 3 material a rating of 0.2.

In both cases, however, the actual rules for Category II and (especially) Category III material at DOE are considerably weaker than those for Category I; it seems likely that the

probability of successful theft at a DOE facility with only Category III protections would be of order ten times as high as that for a DOE facility with Category I protections in place. Hence, in practice, the system advocated here would probably not result in lower levels of protection for Category III material than are in place at DOE. For NRC-regulated facilities or those following current IAEA recommendations, the system advocated here would result in at least somewhat higher levels of protection for Category II and Category III material and therefore a more truly graded, rather than cliffed, system.

The second step in this approach is based primarily on material quality. Some difference in security levels depending on the difficulty of making a bomb from different types of materials, similar to DOE's "attractiveness levels," is justified. Table 4.10 shows proposed discount factors for different types of nuclear material. Nuclear weapons or HEU metal in quantities and enrichment levels suitable for a gun-type bomb would count as the most attractive material, with a discount factor of 1.0. (This differs from DOE's consequence ratings, which assign only assembled weapons a 1.0 consequence rating.) Plutonium or HEU metals suitable for implosion-type bombs would have a discount factor of 0.6. (DOE's consequence ratings make no distinction for the greater difficulty of making implosion-type bombs.) Simple compounds such as oxides that require no elaborate chemical separation to prepare the material for use in a bomb would have a discount factor of 0.8. (The DOE ratings, since they assign only a 0.8 consequence for pure plutonium or HEU metal, to distinguish those from nuclear weapons themselves, use a 0.7 rating for such compounds.) Compounds and mixtures such as MOX, requiring complex chemical separations, would have a discount factor of 0.5 in this approach; the additional difficulty of these separations appears sufficiently large to justify a bigger difference between pure plutonium oxide and MOX, for example, than the small shift from 0.7 to 0.6 in the DOE ratings.

There would be no arbitrary cutoff of 10 weight percent weapons-usable material that would suddenly make such a mixture or compound Category II, as there now is in the DOE system.[266] There would also be no cutoff at 50% enrichment downgrading Category I to Category II material, as there is in the DOE system – though at 40% enrichment and below, material would be considered only suitable for an implosion-type bomb, and the increasing quantity of material needed for a bomb as enrichment declines would be fully reflected, as it is not in current categorization systems.

[266] There may be lower concentrations where a lower discount factor would be justified, if the quantity of material that had to be stolen to get enough for a bomb was so large as to make the theft substantially more difficult to carry out (for example, requiring a vehicle so large as to be difficult to acquire, or a very long period of time to carry the material, or multiple vehicles); alternatively, if a case could be made that the low concentration would lead to a substantially larger processing facility being needed, which would be more likely to be detected, that could also justify a somewhat lower discount factor.

Table 4.10: Proposed Categorization of Nuclear Materials: Quality

Attractiveness Level	Material Type	Discount Factor
A: Weapons and Gun-Type Bomb Materials	Weapons, ≥50 eff. kg HEU metal (>40% enrichment)	1.0
B: Implosion-Type Bomb Materials	Pu metal, < 50 eff. kg HEU metal (>40% enrichment), HEU metal ≤ 40% enrichment	0.6
C: Compounds and Mixes Not Requiring Chemical Separation	Oxides, carbides, nitrates, other direct-use compounds, alloys and mixtures	0.8
D: Compounds and Mixes Requiring Chemical Separation	Alloys and mixes requiring chemical separation; fuel elements and assemblies; solutions	0.5
E: Lightly Irradiated Material	Emitting ~20-400 rad/hr at 1 m	0.8
F: Irradiated Material Requiring Remote Handling	Emitting ~400-10,000 rad/hr at 1 m	0.2
G: Highly Irradiated Material Imposing Disabling Doses During Theft	Emitting >10,000 rad/hr at 1 m.	0.001

Material that was irradiated, but at levels below those needed to impose acutely disabling doses on thieves, or to require recipients to use remote handling, would have a discount factor of 0.8 in this approach. (This contrasts sharply with the DOE approach, in which Category I material emitting even the minimal level of 15 rem/hr at one meter is automatically downgraded to Category II, and material emitting 100 rem/hr at one meter or more is automatically downgraded all the way to Category IV, requiring virtually no physical protection measures.) Material radioactive enough to require remote processing if the recipients are not receive lethal or disabling doses would have a much lower discount factor of 0.2, reflecting the substantial difficulties of processing such material for use in a bomb. Material radioactive enough to disable thieves before they could complete their theft would be considered self-protecting and would have a very small discount factor. Most spent fuel from power reactors would fall into this latter category, with a very small discount factor; but as the radiation field from the spent fuel decayed, decades after discharge, its discount factor would increase, and additional physical protection measures (or passive measures such as emplacement in a difficult-to-access repository) would be needed.

The judgments in the table as to where these thresholds may lie are highly preliminary, intended for illustration, not recommendation: additional research is needed (possibly at the classified level) to make more informed judgments of, for example, the level of radiation that would likely require recipients who wished to avoid lethal or disabling doses to go to remote operations to chemically process the material they had received.

Somewhat difficult issues arise in combining different aspects of material quantity and quality. As discussed above, the chance that an adversary group could successfully make an implosion bomb and the chance that they could successfully separate plutonium from uranium in MOX (to take one example) are not likely to be statistically independent, so it would not be reasonable to simply multiply the 0.6 discount factor for plutonium and the 0.5 discount factor for compounds requiring separation and reach a discount factor of 0.3. In the discussions above, for example, I suggest a discount factor in the range of 0.4 for lightly irradiated uranium-aluminum HEU research reactor fuel, and in the range of 0.36 (0.6 times 0.6) for fresh fabricated MOX fuel assemblies for light-water reactors.

Implementation Issues

What would implementing such an approach mean for the levels of protection afforded to different types of nuclear material, compared to the levels of protection they now receive? In a few cases, security requirements might be reduced; in a larger number of cases, they would be increased.

- Research reactors using 30-70% HEU that are now considered to have a Category I quantity of nuclear material might be downgraded to Category II (if the quantity of material on site was not very large), because of the use of "effective kilograms." This would mean significantly lower security requirements for facilities in this category.
- A substantial number of research reactors that now have modest security arrangements because their fuel is considered to be "self-protecting" at 100 rad/hr at one meter would no longer be able to consider their fuel self-protecting and would have to provide increased protection for it.
- DOE facilities with substantial quantities of HEU that is less than 50% enriched, or materials containing less than 10% by weight weapons-usable material, would have to upgrade from Category II to Category I protections. Similarly, guidance for DOE programs to improve security for nuclear stockpiles in other countries would have to be modified to ensure that such stocks were adequately secured.
- Special consideration would have to be given to the discount factor (and resulting security rules) to be applied to decades-old power reactor spent fuel, as the radioactive barriers to theft and processing decay. In some cases, it may be appropriate to upgrade current protections for such fuel – though in many cases, existing protections against sabotage are likely to be sufficient to protect against plausible theft threats for this difficult-to-steal material.

Summarizing the Proposed Method

The approach to identifying the highest-risk facilities and transport legs outlined in this chapter is conceptually quite straightforward, involving four basic steps:

1. **Effectiveness of security.** First, analysts using this approach would estimate what types of adversary capabilities the security system for a facility or transport leg could defeat,

with what probability (taking into account not only the active security measures but the characteristics of the facility and of the material, as described above).

2. **Level of threat.** Second, analysts would estimate would estimate what types of capabilities outsider and insider adversaries might be able to bring to bear to carry out a theft on a particular facility or transport leg, with what probability, given the country and area where it was located. Combining these assessments of threat and security level makes it possible to make an estimate of the probability that a theft attempt would be successful – that the adversary capabilities would be sufficient to overcome the security measures and steal the guarded material or weapon. Assessments of the level of threat would also be the basis for estimating how the probability of a theft attempt occurring at all varied from one country or area to another.
3. **Utility of material or weapon.** Third, analysts would assess the probability that adversaries who received the material or weapon that could be stolen from that facility or transport leg could gain the ability to detonate a nuclear explosive from them.
4. **Probability of theft attempt.** Fourth, using the answers to the previous three questions, analysts would assess the probability that any type of significant theft attempt would occur at the facility or transport leg in question.

Combined, the probability of a theft attempt, the probability that attempt would be successful, and the probability of successful bomb-making represent the overall risk of nuclear theft for a particular facility or transport leg. With such assessments, it would then be possible to rank the relative risks of nuclear theft and terrorism posed by different facilities and transport legs all over the world and focus policy interventions on those posing the highest present risks.

In essence, in this approach analysts would be attempting, for each facility and transport leg with a nuclear weapon or a kilogram quantity of separated plutonium or HEU, to recreate Table 4.1 (describing the probability of various types of theft attempts, the probability that these various types of attempts would be successful, and the probability of successful bomb-making, for facilities in two hypothetical countries).

While this approach is conceptually simple, it is anything but simple to implement, because complete information that would support highly accurate estimates of these probabilities is rarely available. Nevertheless, informed estimates based on all available sources of information will provide a far better basis for policy decisions than simpler approaches such as those that are currently guiding policy (at least in the United States). These tend to be based only on the stovepipe of a particular program ("we're only doing upgrades in Russia"); or only on the quantity of particular types of material ("we're equally interested in any material that's Category I according to the IAEA definition"); or only on yes/no determinations about compliance with a particular rule ("we're only interested in upgrading facilities that don't meet the IAEA recommendations, we assume security for those that do is good enough").

The practical effect of shifting to this proposed approach from these simpler approaches would be to:

- Highlight the importance of working with particularly high-threat states (such as Russia and Pakistan) to ensure that nuclear stockpiles are protected against larger and more capable threats than is necessary in other countries (and to try to address the terrorism, crime, and corruption problems in those states, so as to reduce the probability of high-capability theft attempts).
- Emphasize the need for high levels of security for particularly attractive materials (such as large quantities of HEU metal) even if they exist in relatively low-threat states.
- Make clear that some materials currently dismissed as posing only minor threats (such as irradiated HEU emitting 100 rad/hr at 1 meter or more) also require significant levels of protection.
- Identify particular areas for collection of additional information to improve the assessments (such as data on indicators of the scale of insider and outsider threats in different countries and the specifics of protections against such threats at different facilities and transport legs).

A First Cut at Applying the Method

Even less of the information needed to make judgments on all of these matters is available in the open literature than is available to the U.S. government or other leading governments. Nevertheless, for the purposes of illustration, it is worth attempting to apply the method proposed in this chapter, at least for a few cases. While the method ultimately has to be applied at the level of individual facilities, it would not be sensible in an unclassified publication to highlight particular named facilities as posing particularly high risks, as that might help adversaries identify good places to attempt to steal from. Instead, in the section below, I will apply the proposed method aggregated at the level of entire countries. I will use Russia, Pakistan, the United States, Japan, Canada, Uzbekistan, and an unnamed developing non-nuclear-weapon state as examples.

Russia and Pakistan are included since a variety of indicators suggest that their nuclear stockpiles face larger outsider and insider threats than any other countries in the world, as will be discussed below. The United States is included because it has some of the most rigorous requirements for nuclear security in the world and because more information is publicly available about the quantity and quality of material at different sites, the security measures at those sites, and the levels of insider and outsider threat than is the case for any other country in the world. The U.S. assessment is broken down into HEU-fueled research reactors and all other facilities with nuclear weapons or weapons-usable materials, because, as discussed above, the NRC's security rules for research reactors are very much weaker than those for any other type of facility with such materials on-site. Japan and Canada are included as examples of countries which have significant stocks of highly attractive weapons-usable material, but where the threats are relatively low (though a strong case can be made that in these days of terrorists with global reach, material of this type in *any* country must be protected at least against certain minimum levels of threat). Uzbekistan is included as an example of a country with very high threats but poor quality nuclear material. The developing non-nuclear-weapon

state is included because the stockpile in question poses one of the higher risks in the developing world; the country is unnamed because it has only one nuclear facility with a noticeable quantity of HEU, and hence a risk assessment for the country overall would, in effect, identify the risks at a particular facility.[267]

Assessing Threat Levels

As described earlier, a full assessment of the threats in a particular country would include an examination of a wide range of information, ranging from the salaries, morale, ideology, and corruption levels among the staff at the particular facilities or transport legs in question to the record of terrorist attacks and major thefts from guarded facilities or transports that have occurred in that country. Such an examination is beyond the scope of this paper. But as also noted earlier, a number of published assessments of terrorism risks, corruption, and related factors in different countries can provide useful, if rough, indicators of the level of threat.[268] Table 4.11 shows, for each of the countries considered here, a rating of terrorism risk;[269] a rating of overall security risk facing firms operating there (a rating that focuses primarily on crime);[270] a rating on corruption level in each country;[271] and an estimate of GDP per capita, adjusted for purchasing power parity (PPP).[272]

---

[267] The particulars of the country and facility are available to qualified researchers on request.

[268] I am grateful to Anthony Wier for his work in compiling a variety of indicators from many sources.

[269] These particular terrorism risk ratings were prepared by the World Markets Research Centre (WMRC), a firm which provides risk analyses to a range of industries, including the insurance industry, in 2003. See Dunn, *WMRC Global Terrorism Index 2003/2004*. This rating of terrorism risk, prepared for use by companies whose profits are riding on the accuracy of their assessments of such risks, appears to be the most complete (in its coverage of countries) and detailed such index that is publicly available. WMRC rated each country on a 1-10 scale on several aspects of the terrorism risk there, including: the motivation of terrorists to attack that country; the presence of active terrorist groups in the country; the scale of terrorist actions that had taken place in the country; the effectiveness of the terrorist groups in that country (that is, how well-organized, well-trained, and well-armed they were); and the quality of the country's efforts at terrorism prevention. After weighting each of these factors, WMRC gave each country an overall rating for terrorism risk; because no country could have a rating of 0 in any category, the possible range of the final scale was 10-100. For the present purposes, terrorists might steal nuclear material in one country in order to attack a different country, so I have modified WMRC's overall ratings by removing the factor of motivation to attack the particular country in question, and then giving equal weighting to each of the four remaining factors. For the countries considered here, this significantly reduces the risk rating for the United States, and reduces the rating more modestly for Canada, Japan, and Uzbekistan, but leaves the ratings for the other countries nearly unchanged. After the preparation of this terrorism index, WMRC was acquired by Global Insight, which provides its analyses only to major corporate clients; there is no public indication that Global Insight has continued the preparation of an annual terrorism risk index.

[270] For this category, the ideal would be to have data on the actual rate of major thefts from guarded facilities in the country, as these are the types of crimes most analogous to nuclear theft. No reliable international data focused on these types of crimes is publicly available, but it is likely that companies working for the insurance industry could compile such data – or make reasonably accurate estimates – and provide this information to governments or international organizations, should governments or international organizations choose to contract for that service. I have not used data on rates of reported crime, as the country-to-country variation in these reported rates seems to be driven as much by differences in the proportion of crimes reported in different countries as by differences in the actual rates of crime. (The most comprehensive publicly available data on reported crime rates is in Office on Drugs and Crime United Nations, *Eighth United Nations Survey of Crime*

None of these are by any means perfect indicators; they are intended to illustrate the approach, not to be definitive judgments of the threats in different countries. The terrorism risk index represents the judgment of one company at one moment in time and was not focused specifically on the risks of the kind of sophisticated assaults that would probably be necessary for an outsider nuclear theft attempt to succeed. The security risk indicator, similarly, is a general estimate, from one company at one point in time, and does not focus specifically on the risk of insider or outsider theft of high-value guarded items. The corruption indicator is one of many developed by different organizations and does not focus specifically on the kinds of corruption most relevant to the threats of concern here – such as corrupt officials granting authorized access to facilities without conducting background checks, or providing security plans to adversaries, or leaving doors unlocked or alarms turned off at pre-agreed times. As noted above, the GDP per capita indicator is only very roughly related to pay at nuclear facilities, as, in countries that devote high priority to nuclear projects, pay at nuclear sites may be far higher than the average; while in other countries, pay at nuclear sites may be lower than per-capita GDP (as was true in Russia in the mid-1990s). Governments or commercial firms supporting the insurance industry would be in a better position to develop indices that specifically assessed the most important risks for each

---

Trends and Operations of Criminal Justice Systems, Covering the Period 2001-2002 (New York: UN, 2005; available at http://www.unodc.org/unodc/en/crime_cicp_survey_eighth.html as of 16 November 2006). While that source tracks the rate of "major thefts" per 100,000 population, data on that variable is unavailable for a number of the key countries of interest, and where it is available, it appears to be incorrect in some cases, reporting, for example, a rate of major thefts in Norway five orders of magnitude higher than the rate in Pakistan.) Some international surveys of crime victims exist, which might provide better data, but they have only been done consistently in a modest number of countries to date. Instead, I have used a rating of the "security risk" facing companies operating in different countries, also compiled by WMRC. Before its acquisition by Global Insight, WMRC published regularly updated estimates of the overall risk companies faced operating in different countries, including ratings for political, economic, legislative, tax, operational, and security risks. The estimate of security risk included both risks from terrorism and risks from crime (and hence there is an overlap with the WMRC terrorism risk rating), but in most countries the risk to companies' operations from major crime far outweighs the risks from terrorism. Since these estimates, as with the terrorism risk estimates, were prepared for companies whose profits depended in part on the accuracy of the assessment (including insurance companies insuring against these risks), this estimate appeared to me the most likely to be reliable of the various rankings of crime risks available. The ratings used here were drawn from an on-line database of *Country Risk Ratings* as of late 2004 (which is no longer available); I can provide the full set of risk ratings for all countries on request.

[271] These ratings are from the international anti-corruption organization Transparency International (TI) and are based on surveys of the perceptions of corruption held by citizens and companies in each country. Because TI uses a rating system in which a high rating means low corruption, I have inverted their 10-point scale by taking 10 minus the TI rating, so that a high rating represents high corruption. See Transparency International, *Corruption Perceptions Index 2004*. There are a variety of different organizations that estimate the scale of corruption in different countries, or the effectiveness of governments in combating corruption; the Transparency International estimates are based on a globally consistent approach, integrate information from a wide variety of other sources, and cover all the countries of most interest, but other ratings could also be used.

[272] World Bank, *World Development Indicators: 2006* (Washington, D.C.: World Bank, 2006). The PPP adjustment – which reflects what a given amount of money can actually buy in different countries – is important because real incomes in many less developed countries are higher than currency exchange rate conversions to dollars would suggest.

Table 4.11: Threat Indicators for Selected Countries

Country	Terror Index (10-100)[a]	Security Risk (1-5)[b]	Corruption (1-10)[c]	GDP/capita, PPP (2004)[d]
Russia	77.5	3.75	7.6	$ 9,097.83
Pakistan	77.5	4.25	7.9	$ 2,044.99
United States	66.25	3	2.4	$ 36,465.05
Japan	45	1.5	2.7	$ 26,883.71
Canada	33.75	1	1.6	$ 28,732.64
Uzbekistan	51.25	3.75	7.7	$ 1,718.30
Unnamed Country	43.75	3.25	5.5	$ 10,471.59

[a]World Markets Research Centre, *WMRC Global Terrorism Index 2003-2004* (London: WMRC, 2003), modified as described in the notes.
[b]World Markets Research Centre, on-line *Country Risk Reports* (London: WMRC, 2003-2004).
[c]Transparency International, *Corruption Perceptions Index 2004* (Berlin: TI, 2004), inverted as described in the notes.
[d]World Bank, *World Development Indicators: 2006* (Washington, D.C.: World Bank, 2006), 2004 incomes in constant 2000 dollars.

country. Nevertheless, these indicators provide a reasonable first cut at highlighting the relative risks in different countries.

The estimated terrorism risk for Russia and Pakistan is higher than for any other states with nuclear weapons or weapons-usable nuclear materials; only Indonesia, with a much smaller quantity of less attractive nuclear material, comes close. This assessment was prepared before the Beslan massacre and the other terrorist attacks of 2004-2006; both Russia and Pakistan would probably rate even higher today. (In my own judgment, the difference in terrorism risk between Russia and Pakistan, on the one hand, and the United States, on the other, is far higher than this particular risk index suggests; both Russia and Pakistan have armed Islamic terrorist movements operating on their territories with a demonstrated capability to launch sophisticated attacks with large numbers of well-armed and well-trained attackers, which is not the case for the United States. Similarly, Uzbekistan's terrorism risk rating, below that of the United States, seems far too low, given the existence of the Islamic Movement of Uzbekistan, a large armed group with close ties to al Qaeda.[273]) Russia, Pakistan, and Uzbekistan also rate very high on security risk, given the scale of crime in those countries, though here Pakistan clearly outpaces the other two. Russia, Pakistan, and Uzbekistan also have more deep-rooted corruption than other countries with nuclear weapons or weapons-usable material, highlighting the possible insider threat. Pakistan and Uzbekistan have far lower levels GDPs per capita than the other countries considered here; even Russia's is one-fourth that of the United States and lower than the developing non-nuclear-weapon state included in this sample.

Japan and Canada, by contrast, both have very low security risk and very low corruption. Japan's somewhat higher rating for terrorism risk may reflect the mid-1990s attacks of the death-terror cult Aum Shinrikyo in Japan. (The cult leaders who organized

[273] This index was prepared well before the unrest in Andijon in 2005; a reassessment today would presumably indicate higher terrorism and security risks.

those attacks have been imprisoned, but the cult, now renamed Aleph, still exists.) The United States rates substantially higher than either Japan or Canada on terrorism risk (given the demonstrated and oft-expressed desire of jihadi terrorists to strike the United States) and on security risk (given the higher rates for major crime in the United States). The U.S. ranking on corruption, like those for Japan and Canada, is quite low. All three countries have high per-capita GDP, offering high salaries for nuclear workers and guards and plentiful resources to provide for nuclear security.

The unnamed developing country has a low rating for terrorism risk, reflecting the lack of organized terrorist activity there in recent years (and its lack of participation in the Iraq war and other U.S.-led initiatives that might make it a target). On the other hand, its ratings for security risk and corruption are fairly high (though not as high as those for Russia, Pakistan, and Uzbekistan), reflecting the high crime rate in the country and the endemic corruption there. Its per-capita GDP is much lower than those of the developed countries in the table, but substantially higher than Uzbekistan's or Pakistan's and even somewhat higher than Russia's, on a purchasing-power-parity basis.

Assessing Overall Nuclear Theft Risks: Two Approaches

Of course, threat levels are only one of the factors to consider in assessing the overall risk of nuclear theft. In what follows below, I will present two approaches to integrating all of the necessary factors into relative risk assessments for different facilities and transport legs in different countries.

The first is based on explicitly attempting to estimate the probabilities of theft attempts with different levels of capability in different countries (and the probability that attempts at those different levels of capability will succeed in overcoming the security systems at particular facilities or transport legs). Both of these estimates involve, in essence, educated guesses – though those guesses are likely to be more reliable in making *relative* assessments between different countries than in making absolute assessments of these probabilities. The second, somewhat simpler, approach is based on rating the threats and the security levels in different countries on a 1-5 scale, based on criteria that are as objective as practicable; in that case, the educated guesses come in attempting to relate these ratings to probabilities of successful nuclear theft.

The first approach is, in effect, based on reproducing Table 4.1 (which describes the risks in hypothetical Country A and Country B) for each facility or transport leg. (Here, as just mentioned, I will be implementing the approach only at the more general national level.) This is a very data-intensive and judgment-intensive approach; only very limited data is available (especially in the public domain) for judging either how likely theft attempts with different levels of capability may be in different countries, or how effective the security systems in different countries would be in defeating those different types of threats. Nevertheless, Table 4.12 presents a first cut at such an assessment, for the sample set of countries listed above. The estimates in Table 4.12 are rounded to one or at most two significant figures; where they refer to a probability of success of 1.0, I do not literally mean

that success is absolutely certain, but only that the chance of failure is small enough to make no noticeable contribution to the overall risk estimate.

Table 4.12 begins with a listing of several ranges of possible adversary capability – identical to that used in Table 4.1. ("Beyond design threats" refers to threat capabilities larger than any of those explicitly described.) For each country, there is then a column containing estimates of the probability that a theft attempt, if it occurred, would be in the specified range of capability; for each country, these estimates sum to 1.0. This is followed by a column containing estimates of the probability that a theft attempt at this level of capability would succeed, given the security arrangements at nuclear facilities with weapons-usable nuclear material in that country. Multiplying these probabilities at each level of capability and summing the result across all the levels of capability gives the overall probability that a theft attempt, should it occur in that country, would be successful, a figure provided in the row below the list of potential levels of capability. The row just below that provides estimates of the probability that a theft attempt will occur at all in each country. (These are intended only as estimates of relative probabilities between different countries; the absolute annual probability of a significant theft attempt in these countries would is almost certainly smaller than the probabilities assigned here.) The next to last row provides the discount factor for the best material in the country in question. Multiplying the probability that a theft attempt would occur in a particular country by the probability that the attempt would be successful and the discount factor gives the overall risk rating, provided in the last row of the table.

Note that in making rough estimates of the likelihood of theft attempts using different levels of capability, I assume that in most cases thieves would try to bring to bear a level of capability they thought would succeed and might often be deterred from attempting a theft if it seemed hopeless. Hence, rather than the highest-probability parts of the distribution being at the most minimal levels of capability, I assume that minimal-capability thieves are often deterred from even launching any significant attempt at nuclear theft, so that the highest probabilities are for bins with some significant chance of success in carrying out a nuclear theft. Since (a) only those attempts involving enough capability to have a significant chance of success contribute to the overall risk, and (b) the purpose here is only to make *relative* rankings of risk between different countries, not *absolute* estimates of how big the risk of nuclear theft is in each country, the low probability assessments for theft attempts with very little capability do not matter much. Only the variance between countries in the estimates of the likelihood of theft attempts with substantial levels of capability affect the estimates of relative risks.

Table 4.12: Estimated Risk of Nuclear Theft in Selected Countries

	Russia		United States		U.S. research reactors	
Threat Level	Att. %	Succ. %	Att. %	Succ. %	Att. %	Succ. %
Beyond design threats	0.1	0.9	0.05	0.8	0.0	1.0
10-15 well-armed outsiders, and/or 1-4 insiders	0.3	0.7	0.1	0.5	0.1	1.0
4-9 well-armed outsiders, and/or 1-2 insiders	0.4	0.5	0.4	0.3	0.5	0.7
1-3 well-armed outsiders, and/or 1 insider	0.15	0.2	0.3	0.1	0.3	0.5
1 unarmed outsider, or 1 poorly placed insider	0.05	0.05	0.15	0.0	0.1	0.1
Prob. theft attempt is successful		0.5		0.24		0.61
Prob. of theft attempt		0.5		0.25		0.25
Discount factor		1.0		1.0		0.4
Relative risk rating		**0.25**		**0.060**		**0.061**

	Pakistan		Canada		Japan	
Threat Level:	Att. %	Succ. %	Att. %	Succ. %	Att. %	Succ. %
Beyond design threats	0.15	0.9	0.03	0.9	0.01	1.0
10-15 well-armed outsiders, and/or 1-4 insiders	0.4	0.7	0.07	0.7	0.05	0.9
4-9 well-armed outsiders, and/or 1-2 insiders	0.3	0.4	0.3	0.5	0.3	0.7
1-3 well-armed outsiders, and/or 1 insider	0.1	0.1	0.45	0.2	0.45	0.3
1 unarmed outsider, or 1 poorly placed insider	0.05	0.05	0.15	0.05	0.19	0.15
Prob. theft attempt is successful		0.55		0.32		0.43
Prob. of theft attempt		0.5		0.15		0.1
Discount factor		1.0		1.0		1.0
Relative risk rating		**0.27**		**0.048**		**0.043**

Source: Author's estimates, explained in the text. "Att. %" refers to the estimated probability of a theft attempt occurring, while "Succ. %" refers to the estimated probability that such an attempt would succeed.

Table 4.12: Estimated Risk of Nuclear Theft In Selected Countries (continued)[a]

	Uzbekistan		Unnamed Country	
Threat Level:	Att. %	Succ. %	Att. %	Succ. %
Beyond design threats	0.1	1.0	0.07	1.0
10-15 well-armed outsiders, and/or 1-4 insiders	0.3	0.8	0.13	0.9
4-9 well-armed outsiders, and/or 1-2 insiders	0.4	0.6	0.4	0.8
1-3 well-armed outsiders, and/or 1 insider	0.15	0.25	0.3	0.5
1 unarmed outsider, or 1 poorly placed insider	0.05	0.1	0.1	0.15
Prob. theft attempt is successful		0.62		0.67
Prob. of theft attempt		0.5		0.3
Discount factor		0.2		1.0
Relative risk rating		**0.062**		**0.20**

Source: Author's estimates, explained in the text. "Att. %" refers to the estimated probability of a theft attempt occurring, while "Succ. %" refers to the estimated probability that such an attempt would succeed.

As noted in Chapter 3, most of the risk of nuclear theft and terrorism comes from the most vulnerable facilities, not only because terrorists and thieves are more likely to succeed if they attempt to steal from these sites, but because they are more likely to pick these vulnerable locations. In Table 4.12, the estimated probability that a theft attempt would be successful follows directly from the estimated chances of attempts at various levels of capability and the chances that attempts at each level would succeed. The probability that such an attempt would occur at all is a judgment; it is higher where threats are higher (clearly such theft attempts are much more likely in Russia than in Japan, for example), reduced somewhat where security is higher and reduced somewhat where the quantity and quality of the material available to be stolen is lower. In what follows, I discuss the ratings for threats, security levels, and quantity and quality of material in Table 4.12, for each of the countries considered.

Russia

Threat. The threat in today's Russia is very high, as discussed in Chapter 2 and in the section on threat indicators, above. Russia is the only country in the world where senior officials have confirmed that terrorist teams are carrying out reconnaissance at nuclear warhead storage sites; some terrorist attacks have involved scores of well-trained suicidal

attackers armed with automatic weapons and explosives, striking without warning; corruption is endemic, as are major insider thefts of non-nuclear items, including from guarded facilities; and while nuclear workers are now paid a living wage, on time, wages for conscript guards at some remote nuclear facilities remain low, and these guards sometimes become "the most dangerous internal adversaries."[274]

Hence, in Table 4.12, I suggest that there is a significant (10%) probability that a theft attempt in Russia would involve a level of capability higher than the highest level specifically described in the table and a large probability (30%) that it would involve the highest level described, 10-15 well-armed outsiders and/or 1-4 insiders. The probability of a theft attempt at the next lower level of capability would be even higher (40%), while the probability of attempts at lower levels of capability would be rather modest (based on the assumption that most potential thieves unable to put together a more substantial theft attempt would be deterred from trying any theft attempt at all).

Security. As discussed in Chapter 2, security for nuclear weapons and materials has improved substantially since the mid-1990s, but significant weaknesses remain. Hence, in Table 4.12, I suggest that while single outsiders and single insiders with no particular plan succeeded in stealing HEU in the mid-1990s, such thieves would have very little chance of success today. Even for a threat of 1-3 well-armed outsiders working with an insider, I suggest only a 20% chance of a theft attempt being successful. But for larger threats, I suggest that the probability of success would increase dramatically.

Quantity and quality of material. Russia has many thousands of nuclear weapons and sites with huge quantities of HEU and separated plutonium, in metal, oxide, and a wide variety of other forms. The discount factor at the sites with the best material (some of which are civilian sites with comparatively modest on-site armed guard forces compared to military sites) is 1.0, the highest possible.

Overall risk rating. With a 50% probability that a major theft attempt would be successful, a 50% probability that such an attempt would occur, and a discount factor of 1.0, Russia gets an overall risk rating of 0.25, in the same range as Pakistan, which is the highest of all the countries in the table. Russia's risk rating is almost four times higher than the rating for the United States. Moreover, two factors that are not considered in this country-rating approach are the huge number of buildings and bunkers where nuclear weapons and weapons-usable materials exist in Russia and the frequent transports that take place there. As discussed in Chapter 3, while the risk of theft does not increase linearly with the number of facilities (because the frequency of theft attempts is determined primarily by the number of groups attempting to get nuclear weapons or materials and the frequency with which they make attempts), more facilities does generally mean more risk, as it means more different groups of people that may include insider thieves and more opportunities for at least one facility to have security weak enough that thieves may observe and successfully exploit the weakness.

---

[274] Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii (Reforming MVD Troops to Guard Russian Nuclear Facilities)," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9, no. 4 (Winter 2003; available at http://www.pircenter.org/data/publications/yk4-2003.pdf as of 28 February 2005).

Hence, if the risks over all the facilities and transport legs in Russia were considered individually and aggregated, the risk would be increased compared to a country with a small number of facilities and few transports, such as Pakistan. This effect – not included in this country-level rating approach – is probably larger than the small difference between Russia's score and Pakistan's score using the methodology shown in the table.

Pakistan

Threat. Both the outsider and insider threats in Pakistan are extraordinarily high, as discussed in Chapter 2. The presence of armed remnants of al Qaeda and the Taliban, along with other highly capable jihadi terrorist groups, along with the frequent terrorist attacks that take place (including the assassination attempts against President Musharraf, some of which have come quite close to succeeding) make clear that high-capability outsider attacks on nuclear facilities are a real possibility. Similarly, the history of the A.Q. Khan network selling highly sensitive nuclear technology across the globe, along with the endemic corruption and insider theft in Pakistan, suggests that major insider theft attempts are a real possibility.

Hence in Table 4.12, the probability of a beyond-design-basis theft attempt (15%) and the probability of a theft attempt at the level of 10-15 well-armed outsiders and/or 1-4 insiders (40%) are both considered to be even higher than in Russia, while the likelihood of attempts involving lower levels of capability is correspondingly lower.

Security. As discussed in Chapter 2, Pakistan's small nuclear stockpile is thought to be heavily guarded, though modern physical protection technologies may not be used. The ratings in Table 4.12 for the probability of success of various types of theft attempt are the same as Russia's for high-capability threats; for lower-capability threats, Pakistan's system is judged slightly more likely to provide effective protection, since it does not have Russia's past record of small threats being able to succeed in defeating the system.

Quantity and Quality of Material. Like Russia, Pakistan has actual nuclear weapons (though Pakistan's are thought to be stored in disassembled form), and substantial quantities of HEU metal. The discount factor at the best sites is 1.0.

Overall risk rating. With a 55% probability that a major theft attempt would be successful, a 50% probability that such an attempt would occur, and a discount factor of 1.0, Pakistan gets an overall risk rating of 0.27, the highest of the countries in the table (though the difference from Russia is easily within the uncertainties of the method). Pakistan's risk rating is over four times higher than the rating for the United States.

United States

Threat. Terrorists are highly motivated to attack the United States, and official assessments suggest that there remains a significant potential for terrorists to operate within the United States. But there is little evidence that large, well-armed, and highly capable terrorist groups are still operating in the United States without detection; since 9/11, the United States has taken a variety of domestic security measures to try to prevent that from happening. Moreover, while there are substantial rates of corruption and major theft in the United States, those rates are much lower than they are in Russia or Pakistan. Nuclear

workers in the United States are far better paid in the United States than in Russia or Pakistan. In short, there is little doubt that the probability of any type of theft nuclear theft attempt is lower in the United States than it is in Russia or Pakistan. Similarly, it seems clear that the probability that an attempt that did occur would involve the highest levels of capability in the table is substantially lower in the United States than it is in Russia or Pakistan. At the same time, however, the possibility of such high-capability theft attempts remains real and the probability of modest-capability theft attempts is probably substantial.

Security. The United States probably spends more on securing its nuclear stockpiles than any other country in the world. At DOE alone, annual security spending (which includes not just physical protection, but also management of secret information, security clearances, and more) is now well over $1 billion per year.[275] DOE facilities with nuclear weapons or weapons-usable nuclear materials are required to be defended against a large, well-armed, and well-trained commando team of outsiders, against insider theft attempts, and against both working together.[276] While important weaknesses remain at some sites,[277] sites such as Pantex and the nuclear weapons storage at Kirtland Air Force Base are probably among the most secure nuclear facilities in the world. Hence, in Table 4.12, even highly capable threats are considered to have a somewhat lower chance of succeeding than they would in Russia or Pakistan, and the probability that low-capability threats would succeed is judged to be quite low.

Nuclear security in the United States is by no means uniform, however. Private Category I facilities regulated by the NRC, not by DOE, are required to defend only against a smaller and less capable DBT, even though the two remaining NRC-regulated Category I facilities both handle large quantities of HEU metal.[278] (A more complete tabulation would treat these facilities separately, with separate security ratings for them.) NRC-regulated nuclear research reactors, as discussed above, are exempt from all but very modest NRC security requirements. The "facility environment" at these sites, however – such as fuel that typically would require tens of minutes to get out of the pool and remove to a waiting vehicle – does, in most cases, provide an additional level of security beyond what is available from the measures specifically designed for physical protection. In Table 4.12, U.S. research reactors (referring primarily to those regulated by the NRC, which are the majority of U.S. HEU-fueled reactors) are treated separately. It seems virtually certain that a high-capability theft attempt at such a research reactor would succeed, and even modest threats would have some chance of success.

Quantity and quality of material. Like Russia, the United States has thousands of nuclear weapons and huge quantities of both HEU and plutonium, in metal, oxide, and many

---

[275] U.S. Department of Energy, *FY 2007 Other Defense Activities.*

[276] While the specific DOE DBT is classified, an informative review of its general characteristics and how they have evolved in the several changes since the 9/11 attacks can be found in Project on Government Oversight, *Y-12 and Oak Ridge National Laboratory at High Risk.*

[277] See, for example, discussion in Project on Government Oversight, *Y-12 and Oak Ridge National Laboratory at High Risk.*

[278] For a discussion of this point, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities.*

other forms. Hence, the discount factor for the main U.S. column is 1.0, the highest possible. NRC-regulated U.S. research reactors, however, are a different story. These facilities typically use fuel where the uranium is mixed with aluminum or other elements, requiring chemical separation before the uranium could be used in a bomb. These facilities never have a Category I quantity of fresh, unirradiated fuel on-site. The fuel in the reactor cores ranges from moderately to highly radioactive; for some reactors, all or nearly all of the fuel in the pool is radioactive enough that the chemical processing would probably require remote handling, though for others this is likely not the case. Only fuel quite recently discharged from fairly high-power reactors would be radioactive enough to be immediately disabling.[279] Overall, NRC-regulated research reactors are considered to have a discount factor of 0.4, corresponding to modestly radioactive HEU in forms requiring chemical separation and in amounts (in most cases) too small for a gun-type bomb with substantial yield.

Overall risk rating. With a 25% probability that a major theft attempt would be successful, a 25% probability that such an attempt would occur, and a discount factor of 1.0, the United States gets an overall risk rating of 0.064, substantially less than that of Russia or Pakistan. More by coincidence than by regulatory intent, NRC-regulated HEU-fueled research reactors end up with approximately the same risk rating, at 0.061, because their far higher probability that a theft attempt would be successful is balanced by their much lower discount factor, reflecting HEU that would require chemical separations before it could be used in a bomb and often has radiation levels in the range of 100s or rem/hr at 1 meter. If adversaries were confident in their chemical processing abilities, they might preferentially choose to attempt to steal material from these less secure sites; in that case, the probability of a theft attempt at these sites would be higher, rather than roughly equal, and the overall risk for U.S. research reactors would be higher than at other sites in the United States.

Canada

Threat. Canada is an example of a comparatively low-threat country. Canada enjoys, in many ways, a more civil society than the United States. In Table 4.11, it is rated as having a lower terrorism risk, lower crime risk, and lower corruption than the United States. On the other hand, Canada is also a good example of the global nature of the threat. There have been cases of terrorist plotting by Islamic extremists in Canada, and with both relatively liberal visa and immigration policies and many thousands of kilometers of effectively deserted border, it would be very difficult for Canada to prevent modest teams of well-trained individuals from entering the country. For these reasons, in Table 4.12**Error! Reference source not found.**, Canada is rated as having probabilities of high-capability theft attempts that are significantly smaller than those in the United States (though still significant), with most of the theft attempt probability clustered at the lower levels of capability. Canada is also rated as having a lower probability that any type of nuclear theft attempt would occur.

---

[279] Calculations provided by Bryan Broadhead, Oak Ridge National Laboratory, suggest that fuel elements from relatively high-power Materials Test Reactor (MTR) or IRT-3M (36% enriched) reactors would continue to have radiation fields that would be acutely disabling (10,000 rad/hr at 1 meter) for over 1,000 hours after discharge, while TRIGA fuel elements might only maintain such a dose rate for some 20 hours after discharge. Personal communication, October 2006.

Security. The modest amount of publicly available information suggests that Canada has significantly increased security for nuclear facilities in response to new concerns following the 9/11 attacks. Prior to those attacks, Canada's published physical protection regulations did not require facilities to have security measures in place capable of defeating any particular DBT; sites were only required to have on-site guards sufficient for tasks such as access control, occasional perimeter patrols, and searches of personnel, not to engage and defeat armed attackers. While there was a general requirement that sites "ensure" that individuals did not bring in explosives or take out nuclear material, searches of individuals were only required when they were justified by "reasonable suspicion" of a particular individual, and there was no specific requirement for portal monitors to detect removal of nuclear materials.[280] Shortly after the 9/11 attacks, the Canadian Nuclear Safety Commission (CNSC, which has responsibility for regulating both nuclear safety and nuclear security) issued orders requiring high-risk licensees (including nuclear power plants and sites with weapons-usable nuclear material) to beef up nuclear security measures, including adding on-site armed guard forces and a variety of other steps.

In the fall of 2006, the requirements of these orders and some additional requirements were incorporated into amended regulations.[281] Now, Canadian nuclear power plants and facilities with Category I and II nuclear material are required to design their physical protection systems "taking into account" a DBT set by the CNSC (as well as credible local threats that may turn up in analyses the licensees are required to do); they are required to have on-site armed guard forces capable of providing "effective intervention" preventing the DBT from succeeding in either theft or sabotage; key personnel are required to have security clearances; access control requirements are much tougher; personnel and vehicles need to be searched for explosives, nuclear material, and other contraband; and so on. The CNSC estimates that meeting the new security requirements cost licensees $300 million in initial capital investments and is costing roughly $60 million per year in increased operating expenses.[282] Today, one key Canadian site with a significant quantity of HEU is reported to have security measures that include searches of all personnel and vehicles, beefed-up access control measures, delay barriers, and an armed "nuclear response force," backed up by troops at a military base not far away.[283]

While these measures have clearly increased security for nuclear materials in Canada, the publicly available evidence does not indicate that the security measures in place are comparable to those at Category I facilities in the United States. There is no publicly available information describing the DBT that the CNSC will require facilities to take into

---

[280] For the text of these pre-9/11 regulations, see Government of Canada, "Nuclear Safety and Control Act: Nuclear Security Regulations," *Canada Gazette Part II* 134, no. 13 (21 June 2000; available at http://canadagazette.gc.ca/partII/2000/20000621/pdf/g2-13413.pdf as of 20 November 2006).
[281] Government of Canada, "Nuclear Safety and Control Act: Regulations Amending the Nuclear Security Regulations," *Canada Gazette Part II -- Extra* 140, no. 4 (7 September 2006; available at http://canadagazette.gc.ca/partII/2006/20060907-x4/pdf/g2-140x4.pdf as of 20 November 2006).
[282] Government of Canada, "Nuclear Safety and Control Act: Regulations Amending the Nuclear Security Regulations," p. 27.
[283] Ian McLeod, "Bombs Away: Forty-Five Kilograms of Bomb-Grade Uranium Are Stockpiled at Chalk River, Awaiting the Long-Delayed Startup of Two Nuclear Reactors," *Ottawa Citizen*, 17 June 2006.

account, but it is very unlikely that these facilities will be required to defend against a threat as challenging as those DOE facilities are now required to defend against. Although the new rules require facilities to conduct "security exercises" every two years (involving both on-site and off-site response forces), they do not include a requirement for realistic force-on-force tests of the ability of the security systems to defeat the DBT (or comparable realistic tests of insiders' ability to smuggle material out); the CNSC is reportedly considering requiring such tests.[284] In many respects, the Canadian regulations are much less specific than those that exist in the United States.

Overall, in Table 4.12, the security measures in Canada are rated as being somewhat less able to defeat various levels of threat than those in the United States (other than at NRC-licensed research reactors), but roughly comparable to the security measures now in place in Russia.

Quantity and quality of material. Most sites in Canada have only modest quantities of weapons-usable nuclear material. A small number of locations, however, have tens of kilograms of fresh, unirradiated HEU.[285] This material deserves a discount factor of 1.0 or close to it.

Overall risk rating. With a 32% probability that a major theft attempt would be successful, a probability of only 15% that such an attempt would occur, and a discount factor of 1.0, Canada gets an overall risk rating of 0.049, significantly lower than that for the United States – in essence because the reduction in threat levels in moving from the United States to Canada is judged to be somewhat larger than the reduction in security levels.

Japan

Threat. Japan perceives itself as a civil society where firearms have been outlawed for hundreds of years and large-scale armed attacks are almost inconceivable.[286] Part of this perception is undoubtedly correct: with Japan's ethnic homogeneity and traditions of communal cooperation, it would be very difficult for any substantial armed group of non-Japanese individuals to enter Japan and operate there. As shown in Table 4.11, Japan is rated as having lower terrorism risks, crime risks, and corruption than the United States.[287] But it

---

[284] Ian McLeod, "How to Keep Nuclear Sites Safe: Stage Mock Terror Attacks: Chalk River Considers U.S.-Style Security Drill," *Ottawa Citizen*, 17 June 2006.

[285] See, for example, McLeod, "Bombs Away."

[286] See, for example, H. Kawai, H. Kurihara, and M. Kajiyoshi, "Physical Protection of Nuclear Material in Japan," in *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations: Proceedings of an International Conference, Vienna, 10-14 November 1997* (Vienna: International Atomic Energy Agency, 1997). This article asserts, as of two years after the Aum Shinrikyo attacks, that "Japan is still the safest country in the world," and provides a table listing underlying factors such as the ban on private possession of swords and firearms, the registration of all citizens and families, and the lifelong employment system as "the premise for considering physical protection of nuclear material in Japan." Similarly, in an interview in November 2006, a senior Japanese physical protection regulator expressed the view that while insider threats at Japanese nuclear facilities were possible, his "personal view" was that armed outsider attack at these facilities was "not credible."

[287] Japan does score higher in several of these respects than Canada, but some of those ratings may not be justified. It seems difficult to argue, for example, that facilities in Canada, with a number of incidents involving

should also be remembered that Japan was the homeland of the Japanese Red Army in the 1970s-1980s, and of Aum Shinrikyo, the terror cult that launched the nerve gas attack in the Tokyo subway in the 1990s – and established an entire factory to manufacture AK-47s. (The key leaders who organized those 1990s attacks were imprisoned, but the cult itself continues to exist, under the new name Aleph.) Japan is also the home of brutal organized crime groups known collectively as the *yakuza*. Moreover, most of Japan's nuclear facilities with weapons-usable nuclear materials are on the seacoasts, where foreign attackers might well arrive by boat with little warning (though how they would elude pursuit after an attack is not clear). Japan's strong communal traditions – and lack of sympathy for jihadi ideologies – reduce the insider threat, but at the same time, they tend to create an atmosphere in which insiders are trusted, with few specific measures in place to address insider threats, creating opportunities for any bad apples that do exist.

Overall, in Table 4.12, Japan is rated as having a lower threat level than any of the other countries considered, with a very small (1%) chance that a theft attempt would be beyond any of the categories of capability described and only a 5% chance that it would be in the highest described category of capability.

Security. Japan, like Canada, significantly strengthened security for nuclear facilities after the 9/11 attacks, but Japan's security upgrades appear not to have gone as far as Canada's.[288] In particular, immediately after 9/11, Japan added armed guards at its nuclear facilities (who were not present previously);[289] in late 2005, new physical protection regulations went into effect that, for the first time, require facilities to "take into account" a DBT specified by the Japanese regulators in designing their nuclear security systems; create a program of inspection of physical protection for the first time; and create, for the first time, an obligation to keep nuclear security information confidential.[290] The limited information publicly available suggests that significant weaknesses in the Japanese physical protection program remain, however.

---

home-grown jihadi extremists in recent years, face a substantially lower terrorism risk than facilities in Japan, but the WMRC terrorism risk rating is lower for Canada.

[288] For a useful discussion of physical protection in Japan before the 9/11 attacks, including the lack of armed guards at nuclear facilities and the absence of any specific measures to address insider threats, see Hiroyoshi Kurihara, "The Protection of Fissile Materials in Japan," in *A Comparative Analysis of Approaches to the Protection of Fissile Materials: Proceedings of the Workshop at Stanford University, July 28-30, 1997* (Livermore, Cal.: Lawrence Livermore National Laboratory, 1997). For other discussions, see Kawai, Kurihara, and Kajiyoshi, "Physical Protection of Nuclear Material in Japan"; H. Nakata, T. Misaka, and H. Tsuruta, "Experience in the Implementation of Physical Protection Measures of Nuclear Material at the JAERI Tokai Establishment," in *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations: Proceedings of an International Conference, Vienna, 10-14 November 1997* (Vienna: International Atomic Energy Agency, 1997).

[289] See, for example, Tatsujiro Suzuki, "Implications of 09/11 Terrorism for Civilian Nuclear Industry and Its Response Strategy," paper presented at Japan Atomic Industrial Forum-Harvard University Nonproliferation Workshop, Cambridge, Mass., 30-31 January 2002.

[290] For a summary of the amended Japanese physical protection law, see Shin Aoyama, "Current Nuclear Physical Protection Measures in Japan," paper presented at Seminar on Strengthening Nuclear Security in Asian Countries, Tokyo, 8-9 November 2006. For a brief critique from a Japanese source, see Hiroshi Masumitsu, "Revised N-Law Inadequate to Cover All Terrorism Scenarios," *Daily Yomiuri*, 18 June 2005.

Under Japanese law, private individuals, including employees of nuclear facilities, are not allowed to have firearms. Shortly after 9/11, therefore, the ministries responsible for nuclear energy asked the heads of the national police and the coast guard to provide armed guards for nuclear facilities (and armed boats to patrol off-shore), which they agreed to do, at their own ministries' expense. These guards remain at Japanese nuclear facilities at this writing, but are not required by any law or regulation; they could be removed at any time the leaders of the national police and coast guard decide that they no longer wish to have their ministries bear the costs of this form of protection.[291] Moreover, these guards are modest in number, largely patrol at the perimeters of facilities (where they might be quite vulnerable to being shot in the opening moments of an attack) and are not integrated into site security plans. Information on the adequacy of their armament, armor, and training in tactical response is not publicly available.

The guards who are employees of the facilities and included in site security plans are armed only with nightsticks.[292] These guards perform functions such as searching personnel and vehicles (a process that has been greatly stepped up in recent years), access control, manning central alarm stations, alarm assessment, and checking the perimeter for vulnerabilities. The sites' security plans for defeating the DBT still rely primarily on off-site response forces, since the armed guards from the national police are not integrated into security plans.[293] Yet in some cases the first fence with intrusion detection in place is only a 10-30 meters from the building where nuclear material exists, suggesting that unless there are very sophisticated multi-layer delay systems within the building, the time it would take after detection for well-trained attackers to get into the material area, steal the material, and depart may be smaller than the time it would take off-site response forces to arrive.[294]

There continue to be few explicit measures taken to address insider threats in Japan. In particular, because of privacy concerns in investigating employees of private institutions, no background checks are performed on employees of nuclear facilities, even those who are guards or who have direct access to weapons-usable nuclear material.[295] On the other hand, technological measures such as portal monitors when entering or leaving nuclear facilities are in place.

Overall, Japanese regulators estimate that meeting the new physical protection regulations has cost licensees – both nuclear power plants and facilities with weapons-usable nuclear material – a total of some $50 million. Most of this rather modest sum has gone for adding additional unarmed guards.[296] In stark contrast to the situation in the United States, maintaining a building as a Category I facility is apparently not very expensive. For example, at one large nuclear site with major plutonium facilities, there is a small building with critical

---

[291] Interview with Japanese physical protection regulator, November 2006.
[292] See, for example, Masumitsu, "Revised N-Law Inadequate to Cover All Terrorism Scenarios." This was confirmed in an interview with Japanese physical protection regulator, November 2006, and personal observations on a visit to a Category I nuclear facility, November 2006.
[293] Interview with Japanese physical protection regulator, November 2006.
[294] Author's observations from a visit to a Category I nuclear facility in Japan, November 2006.
[295] Interview with a manager at a Japanese Category I nuclear facility, November 2006.
[296] Interview with a Japanese physical protection regulator, November 2006.

assemblies, where more than a significant quantity of plutonium is stored. Although funds are not available to make any use of this plutonium in the near term, no one has bothered to move it to one of the major plutonium facilities less than five minutes away on the same site, so that the critical assembly building would no longer require Category I protection.[297]

Material quantity and quality. While most of Japan's separated plutonium stocks are located in France and the United Kingdom, Japan has tons of separated plutonium on its own soil.[298] In addition, Japan has hundreds of kilograms of weapon-grade HEU, a substantial amount of it in metal form.[299] The material at some Japanese sites deserves a discount factor of 1.0, the highest possible.

Overall risk rating. With a 43% probability that a major theft attempt would be successful, a probability of only 10% that such an attempt would occur, and a discount factor of 1.0, Japan gets an overall risk rating of 0.043 – roughly similar to Canada's, as a higher probability that a theft attempt would be successful (resulting from weaker physical protection measures) is balanced by a lower estimated probability that a theft attempt would occur (given the generally low state of the threat in Japan). This represents the lowest overall risk rating in the table. Given that key elements of the estimate, particularly the relative probability of a theft attempt being made, are little more than educated guesses, this low risk rating should be taken with considerable caution. As noted at the outset, especially where risk estimates are quite uncertain, policy should be risk-informed, not exclusively risk-based. The estimated probability that a theft attempt would be successful in Japan is far higher than it is in the United States, and some of Japan's material is extremely high quality: the risk estimate is low only because of a low estimated chance that a major theft attempt will occur in Japan. Wherever it may be in the world, very high quality material should have security sufficient to reduce the probability that a theft attempt would succeed to a very low level, even if the best guess is that the probability of such an attempt occurring in that country is modest.

Uzbekistan

Threat. The threat in Uzbekistan is very high. The Islamic Movement of Uzbekistan is a well-armed terrorist group closely linked to al Qaeda. The bloody crackdown in Andijon in May 2005 was preceded by groups of armed individuals seizing control of a military

---

[297] Author's observations from a visit to a Category I nuclear facility in Japan, November 2006. Specifics of the facilities involved available to qualified researchers on request.

[298] As of the end of 2005, there were more than 5 tons of separated plutonium on Japanese soil, and more than 37 tons of Japanese separated plutonium stored abroad. See International Atomic Energy Agency, *Communication Received from Japan Concerning Its Policies Regarding the Management of Plutonium*, INFCIRC/549/Add.1/9 (Vienna: IAEA, 2006; available at http://www.iaea.org/Publications/Documents/Infcircs/2006/infcirc549al-9.pdf as of 21 November 2006).

[299] See, for example, David Albright and Kimberly Kramer, "Civil HEU Watch: Tracking Inventories of Civil Highly Enriched Uranium," in *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, 2005; available at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html as of 21 July 2005).

garrison (where they seized a large number of weapons), a police station, and a prison.[300] There seems little doubt that a similar group would have been able to seize control of a nuclear research reactor should they have chosen to do so. Uzbekistan's rating for terrorism risk in Table 4.11 is lower than that for the United States, which appears unjustifiable; it seems clear that the terrorism risk in Uzbekistan is high, though perhaps not quite as high as the risk in Russia or Pakistan (given the Uzbek government's brutal suppression of such activities). As shown in Table 4.11, Uzbekistan's ratings for security risk and corruption are very high, and its GDP per capita is below even that of Pakistan. Hence, in Table 4.12, the probabilities of the various levels of high-capability theft attempts and the probability that a theft attempt would occur at all in Uzbekistan, are rated as being equal to Russia's. This may somewhat exaggerate the likelihood of a theft attempt in Uzbekistan, however, as it does not take into account the poor quality and quantity of the material available to be stolen there, which might affect target selection by potential thieves.

Security. Like other non-Russian states of the former Soviet Union, Uzbekistan had only modest and antiquated security measures in place at its civilian nuclear sites when the Soviet Union collapsed and a government with no previous experience in physical protection. Since then, with U.S. and other international funding and assistance, Uzbekistan has drastically improved the security measures at sites with HEU. The first round of internationally-financed physical protection upgrades at Uzbekistan's main research reactor was declared completed in 1996.[301] These upgrades were designed to meet IAEA physical protection recommendations (INFCIRC/225), which were then in their third revision. In September 2000, following terrorist attacks by the IMU in Tashkent, the president of the Uzbekistan Academy of Sciences sent an urgent request to the U.S. government for assistance with further upgrades at this reactor site.[302] Further upgrades were also needed to comply with the fourth revision of INFCIRC/225, issued in 1999. This second round of U.S.-sponsored upgrades, completed in 2002, included installing a new fence with intrusion detectors, a new external access control site, replacing wooden interior doors with doors designed for high security, and more.[303] The site now has a modern double fence with intrusion detection, portal monitors, security cameras, a protected central alarm station, and on-site armed guards.[304] Information is not publicly available on the kinds of threats the site's security system and guard forces (backed up by whatever off-site forces could respond in time) could defeat, or on the measures in place to address insider threats. U.S.-sponsored

---

[300] For an official description of these events, see, for example, U.S. Department of State, *Country Reports on Human Rights Practices: 2005* (Washington, D.C.: U.S. Department of State, 2006; available at http://www.state.gov/g/drl/rls/hrrpt/2005/ as of 22 November 2006).

[301] U.S. Department of Energy, *Improving Nuclear Materials Security at the Institute of Nuclear Physics - Tashkent, Uzbekistan* (Washington, D.C.: DOE, 1996; available at http://www.nti.org/e_research/profiles/Uzbekistan/index_6084.html as of 2 June 2006).

[302] "Physical Protection Upgrades for the Uzbekistan VVR-SM Reactor," *International Security News* 2, no. 2 (May 2002; available at www.cmc.sandia.gov/isn/may02isn.pdf as of 22 November 2006), pp. 14-15.

[303] "Physical Protection Upgrades."

[304] Some of these measures are described, for example, in Holbay Halilov, "Minimizing Security Risks in Uzbekistan," paper presented at Seminar on Strengthening Nuclear Security in Asian Countries, Tokyo, 8-9 November 2006.

physical protection upgrades at a second site in Uzbekistan with a small amount of HEU were completed in fiscal year 2005.[305]

Overall, in , Uzbekistan's physical protection measures are judged to be slightly more effective in defeating various levels of threat than Japan's, but slightly less effective than Canada's. (The uncertainties in all of these judgments are larger than the estimated differences between these countries.)

Material quantity and quality. The United States, Russia, Uzbekistan, and the IAEA have cooperated to remove most of the HEU from Uzbekistan, leaving relatively modest stocks of fairly poor-quality material remaining. Shipment of approximately 63 kilograms of uranium in irradiated HEU research reactor fuel back to Russia was completed in April 2006 (including a substantial quantity of fuel that had originally been 90% enriched, along with material that had originally been 36% enriched).[306] Roughly 3 kilograms of fresh HEU had been shipped back to Russia in September of 2004.[307]

The HEU remaining in Uzbekistan includes in-core material in its two research reactors and presumably also a modest amount of irradiated fuel that was not yet cool enough to ship in April 2006. There may also be a modest amount of fresh fuel for use before the reactors' planned conversion. One of Uzbekistan's research reactors is a pulse reactor with uranium in a liquid solution, reportedly containing several kilograms of 90% HEU in the solution; this would be a Category II quantity in either current IAEA categorizations or the categorization proposed above. Since a pulse reactor generates a modest total number of fissions, this material is not very radioactive. But stealing it would not be trivial to do: it would require figuring out how to drain the solution from the reactor core, carry it away, and recover the HEU from the solution.

The other Uzbek research reactor now operates on 36% enriched fuel. A typical loading would include somewhat more than 5 kilograms of U-235 in HEU that was originally 36% enriched (though at any given time, a smaller amount of U-235 would still be present in the core, as some of it would have been consumed).[308] This represents just under 2 effective

---

[305] Data provided by DOE, December 2005. Names and locations of relevant facilities available to qualified researchers on request.

[306] U.S. Department of Energy, National Nuclear Security Administration, "Secret Mission to Remove Highly Enriched Uranium Spent Nuclear Fuel from Uzbekistan Successfully Completed: Four Shipments Have Been Sent to a Secure Facility in Russia" (Washington, D.C.: NNSA, 27 September 2006; available at http://www.nnsa.doe.gov/docs/newsreleases/2006/PR_2006-04-20_NA-06-10.htm as of 16 May 2006). For a table of how many 90% and 36% assemblies were included in each shipment, see Halilov, "Minimizing Security Risks in Uzbekistan."

[307] "Secret Mission to Recover Highly Enriched Uranium in Uzbekistan Successful: Fuel Returned to Secure Facility in Russia" (Washington, D.C.: U.S. Department of Energy, 13 September 2004; available at http://www.energy.gov as of 16 February 2005).

[308] A typical core loading includes 18 assemblies which each contain 300 grams of U-235. See N. A. Hanan et al., "Feasibility Studies for LEU Conversion of the Wwr-SM Reactor in Uzbekistan Using Pin-Type and Tubular Fuels," in *Proceedings of the 25th International Meeting on Reduced Enrichment for Research and Test Reactors, Chicago, Ill., 5-10 October 2003* (Argonne, Ill.: Argonne National Laboratory, 2003; available at http://www.rertr.anl.gov/RERTR25/PDF/Hanan.pdf as of 22 November 2006). I am grateful to Ethan Stillman for research on the nuclear facilities in Uzbekistan, including locating this reference.

kilograms (even not taking account of the burnup of U-235), making this a Category II quantity of material in the categorization system proposed here, even if it were not radioactive. Since the reactor has a thermal power of 10 megawatts and reportedly is heavily used (with more than 6,000 hours of reactor operation per year), much of the in-core material would be quite radioactive, certainly enough so to require remote processing, even if it were not radioactive enough to be immediately disabling during the course of a theft. Similarly, any discharged fuel not yet shipped is likely to be modest in quantity; its remaining enrichment level is likely to be in the 20-25% range; and it is likely to be radioactive enough to require remote processing, though not radioactive enough to be disabling during a theft.

In short, the nuclear material that remains in Uzbekistan is not very attractive: it is predominantly in reactor cores; it is not in Category I quantities; and it is either in a difficult-to-remove solution or it is only medium-enriched and quite radioactive. Overall, I assign a discount factor of 0.2 to the best remaining Uzbek material.

Overall risk rating. With its very high threat and moderate security measures, Uzbekistan has one of the highest estimated probabilities that a nuclear theft attempt would be successful (62%) on in Table 4.12, along with a high estimated probability that a theft attempt might occur. But with only modest quantities of relatively low-quality material, the overall risk rating is 0.062, comparable to the remaining risk at the well-protected facilities at DOE in the United States. Even that risk rating may be too high, as it may be that the probability of a theft attempt should be lower, given the modest contribution to an adversary nuclear weapons effort that theft from these facilities would make. Prior to the recent removals of material from Uzbekistan, however, the overall risk was far higher: the material recently removed included a substantial quantity of irradiated fuel that had originally been 90% enriched (and was probably still in the range of 80% enrichment), much of which was probably not emitting even 100 rem/hr at 1 meter. Hence, that recent removal operation made a dramatic difference in reducing a particularly urgent risk of nuclear theft. Although the remaining risk in Uzbekistan is moderate, it remains important to convince Uzbekistan to convert these reactors to LEU if they are still needed, or shut them if they are not, and remove the last of the HEU – both because the remaining HEU still poses some risk, and because the high-power reactor will require regular shipments of fresh HEU (and generate increasing quantities of irradiated HEU) as long as it continues to operate with HEU fuel.

Unnamed Country

Threat. Like Uzbekistan, the rating for terrorism risk in Table 4.11 for the unnamed developing country – which is slightly lower even than Japan's – seems unreasonably low. This country has little recent record of major terrorist activity, but it is difficult to argue that the terrorism risk there is not higher than the risk in Japan. The country has wide disparities of wealth, with many living in grinding poverty; a range of ethnic groups competing for political power and resources; widespread possession of guns; and relatively lightly-controlled borders and rural areas, increasing the possibility that terrorist operatives from outside could operate there. As shown in Table 4.11, the country has high crime risks and substantial corruption (though the latter is not quite as severe as in the cases of Pakistan,

Uzbekistan, and Russia). It has a moderate per-capita income, roughly comparable to Russia's.

Overall, as shown in Table 4.12, I estimate that the probabilities of the highest-capability categories of nuclear theft attempt in this country are modestly higher than those in the United States, though lower than those in Russia. Similarly, I judge the probability of any type of nuclear theft attempt taking place in this country to be somewhat higher than the probability in the United States, but substantially lower than the probability in Russia.

Security. The major site with HEU in this country does have a perimeter fence and on-site guards. Site reviews by foreign experts, however, have concluded that the security at the site does not meet IAEA recommendations, and U.S. officials consider security upgrades at this site to be a matter of some urgency.[309] Hence, in Table 4.12, I have rated the security measures in this country as having modestly less chance of stopping theft attempts at each level of capability than the measures in place in Japan have. In general, however, very little information about the specifics of the physical protection arrangements in this country is publicly available.

Material Quantity and Quality. There are hundreds of kilograms of HEU at this country's one major site with weapons-usable nuclear material, much of it in metal form. Hence, this country's material rates a discount factor of 1.0.

Overall risk rating. This country has a moderate to high threat and modest security measures, leading to a 67% estimated probability that a nuclear theft attempt, if made, would be successful – comparable to the probability for Uzbekistan, or for U.S. research reactors. But the material available in this country is much higher quality than the material in Uzbekistan or at U.S. research reactors: with a discount factor of 1.0, the overall risk rating is 0.20, almost as high as those for Russia and Pakistan.

In short, in this approach to rating relative risks, Russia and Pakistan leap out as posing higher risks than the other countries, despite having substantial security measures in place, because of the immense threats there. Efforts to reduce risks in those countries should focus not only on strengthened security measures at nuclear sites, but just as importantly (if not more so), on programs to reduce both insider and outsider threats, through improved counter-terrorism and anti-corruption programs, among other measures. The unnamed country also poses a particularly high risk, despite its more moderate threat environment, because of its comparatively weak security measures and the high quality of the material there. Uzbekistan posed almost a comparable level of risk (because, again, of the immense threats there) until its best nuclear material was removed, but now poses a significantly lower risk because of the small quantity and poor quality of material remaining at its sites with HEU. This makes clear that the recent removals of material from Uzbekistan were major successes in risk reduction.

By this estimate, the well-protected sites in DOE's complex in the United States pose only a moderate risk, despite the high-quality material there; NRC-regulated research reactors

[309] Interview with DOE officials, October 2006.

pose a far higher probability of successful nuclear theft, because of their weak security measures, but a similar estimated overall risk, given the lower quality of material available to be stolen at such sites. Canada and Japan both appear to pose relatively low risks, largely because of the low threats in these countries; Japan in particular, however, continues to have fairly modest security measures in place, and if a theft attempt with high levels of capability *did* occur, its probability of success would be distressingly high. That latter point emphasizes the large uncertainties in these assessments: if, for example, the probability of a theft attempt occurring at all in Canada or Japan turned out to be higher than estimated here, the estimate of the risk posed by these countries' nuclear stockpiles could increase very substantially. The same can be said for, for example, U.S. HEU-fueled research reactors (or those with similar levels of security in other countries): if the probability of a theft attempt at these sites were judged to be higher because of the higher probability of success, compared to better-defended sites, then the overall risk they pose could be substantially higher than that estimated here.

The second, rating-based approach involves establishing a set of criteria by which to give facilities and transport legs (or entire countries, as in this example) ratings for both the threat they face and the effectiveness of their security arrangements. I have chosen to use a 1-5 scale in both cases (with one being the lowest and five the highest). I then provide a very rough estimate of how the probabilities of theft attempts and of those attempts being successful, relate to the differences between the threat rating for one location and the security rating for that location. Combined with the discount factors for the materials available to be stolen, this again offers the opportunity to estimate overall risks of nuclear theft at different locations. First, I describe proposed criteria for different threat and security ratings.

In assessing the level of threat in different countries:

- A country with a rating of "5," the highest level of threat, would be expected to be one that has large and highly capable terrorist groups operating on its soil; where multiple large terrorist attacks have taken place; where corruption and insider theft (or insider participation in terrorist conspiracies) is high; and where either per-capita GDP is below $3,000 per year, or there are other indications that pay for nuclear workers and guards is low enough to provoke at least intermittent desperation.
- A rating of "4" would correspond to a country with capable terrorist groups operating on its soil; where multiple terrorist attacks have taken place; where corruption and insider theft is above average, compared to other countries; and where either per-capita GDP is below $10,000 per year, or there are other indications of low pay for nuclear workers and guards.
- A rating of "3" would correspond to a country with at least some record of terrorist groups on its soil in recent times; where at least one or two significant terrorist attacks have taken place; where corruption and insider theft is roughly average compared to other countries; and where per-capita GDP is below $20,000 per year.
- A rating of "2" would correspond to a country with only few and modest cases of terrorism on its soil in recent times; where corruption and insider theft are below average, compared to other countries; and where per-capita GDP was above $20,000 per year.

- A rating of "1" would correspond to a strongly socially cohesive country, with little or no record of terrorism, very low levels of corruption and insider theft, and per-capita GDP above $20,000 per year (above that level, it appears unlikely that further increases would much reduce the chance of desperation driving theft – and if sheer greed is the driver, even much higher pay may not solve the problem). Realistically, in the current age of terrorists with global reach, a "2" is probably the lowest rating that can be justified for any country.

While most of these factors are at least somewhat judgmental, this system provides a framework in which generally consistent judgments about the relative risks in different countries can be made. The threat variables mentioned do not always vary together, so some countries may have some variables in one category and others in another. If several variables together are in a high-threat category, the country deserves that high-threat ranking, even if one or two are in a lower-threat category.

In assessing the level of security in different countries:

- A country with a rating of "5" would be expected to require its nuclear facilities to have: security measures in place capable of defeating a highly capable DBT including both outsiders and insiders, good training and information, and a wide range of weapons and tactics; a rigorous regulatory system for nuclear security, including detailed inspections, realistic tests of the systems' performance in defeating both insider and outsider threats, and effective enforcement; effective approaches for investigating and monitoring the trustworthiness of all personnel with important roles in nuclear security and limiting access to key areas to such cleared personnel; well-armed and well-trained on-site guards, coupled with tested procedures in place for local police or military forces to provide backup in the event of an emergency; extensive police and intelligence efforts focused on preventing nuclear terrorist conspiracies; sufficient resources allocated so that all security measures required by regulations can be taken in a timely way; and an effective process in place for regularly reviewing and adapting its approaches on the basis of experience and changing threats.
- A rating of "4" would correspond to a country that has a regulatory DBT in place (or a rule-based system resulting in comparable performance), including both outsider and insider threats, but a threat that is somewhat less capable than would be the case for a state rated "5" (for example, possibly including fewer attackers, or less capable weaponry, or less access to inside information on the site's security system). A country with a rating of "4" would be expected to have: a system of nuclear security regulations in place (including both inspections and enforcement); some process for background checks on personnel granted access to weapons-usable nuclear material or charged with guarding such material; some armed on-site guards, coupled with tested procedures in place for local police or military forces to provide backup in the event of an emergency; at least modest police and intelligence efforts focused on preventing nuclear terrorist conspiracies; and resources allocated that are generally sufficient, but sometimes require important security measures to be foregone or postponed.

- A rating of "3" would correspond to a country whose nuclear security systems are designed for reasonable performance against at least modest threats. A country with a rating of "3" might have: no regulatory DBT, but instead have a rule-based regulatory approach (compliance with which would provide reasonable protection against modest threats); a weak, but not totally ineffective, system of inspections and enforcement; and some process for background checks on personnel granted access to weapons-usable nuclear material or charged with guarding such material, though possibly with significant gaps. Such a country might have small numbers of armed guards at nuclear sites, but they might not be very well-armed or well-trained, or be well-integrated into the site security plans; there would likely be some planned procedure in place for local police or military forces to provide backup in the event of an emergency, but it might not have been very well-planned or tested, and these backup forces might not be especially well-armed, well-trained, or numerous either. There would probably be little police and intelligence efforts focused on preventing nuclear terrorist conspiracies, and cases where security measures were not taken because of lack of resources would occur regularly. A country rated "3" would usually comply with IAEA physical protection recommendations.
- A rating of "2" would correspond to a country with some basic nuclear security measures in place, but where these measures would, at best, be able to protect against a very modest number of armed outsiders (2-3) or one insider without an effective plan. There would likely be some nuclear security regulations in place, but they would have major weaknesses, and there would typically be no regulatory DBT; inspections might be neither frequent nor effective; the regulatory agency might lack the power and independence required for tough enforcement. On-site armed guards might range from zero to one or two lightly armed individuals, and arrangements for armed response from off-site would typically be weak. Measures to check the trustworthiness of individuals before granting them access to nuclear material or a role in guarding such material might be cursory or nonexistent. Such a country would typically have many cases where important security measures were not taken because of lack of resources. Some facilities might comply with IAEA physical protection recommendations, others might not.
- A rating of "1" would correspond to a country where at least some nuclear facilities with potential nuclear bomb materials have very few security measures in place. In a country rated "1", there might be: no fences at all around such facilities, or fences with gaping holes; no on-site armed guards at nuclear facilities and no recently-tested arrangement for rapid armed response from off-site; an absence of portal monitors to detect unauthorized removal of HEU or plutonium and of security cameras to monitor activities in nuclear material areas; few measures in place for checking the trustworthiness of key personnel before hiring them, or monitoring trustworthiness afterward; and nuclear material accounting systems that would not be capable of detecting a substantial theft in a timely way. A country rated "1" would clearly not comply with IAEA physical protection regulations.

As with the threat ratings, these variables may vary independently; countries may not fit the entire description for a particular rating perfectly. Some countries, for example, may

have a heavy reliance on armed guards but little application of modern security technologies and few detailed regulations. Other countries may have an extensive regulatory infrastructure, a great deal of technology in place, but be weak on armed response to potential threats. Moreover, the publicly available information on which to rate the security systems in different countries is quite limited. (Here, too, governments, with access to classified assessments and a broader range of actual visits to facilities in many countries, would be in a better position to provide accurate ratings; those used here are only intended to be illustrative.) As with the threat ratings, a substantial degree of judgment is inevitably involved.[310]

There is no rigorous means of converting these threat and security ratings into probabilities of nuclear theft; only educated guesses as to the likely relationship are possible. Again, however, for estimates of *relative* risks between different facilities, these estimates may be somewhat less problematic than they would be for making estimates of the absolute magnitude of risks from different facilities – and they are surely better than not even attempting to take a risk-based approach. Here, I use two roughly estimated factors to translate the ratings into relative risk estimates. In this approach, the "attempt probability factor" is based solely on the threat level: in states with higher threats, there will be higher probabilities of a nuclear theft attempt being made. The "attempt probability factor" is simply the threat rating divided by ten. A more sophisticated approach would also include security levels at sites (taking into account that theft attempts might well be deterred by high security levels, or that opportunistic thieves might be tempted by very low security levels), and also the discount factor (taking into account that thieves would be less likely to attempt to steal material that would be very difficult to make a bomb from). Yet there is reason to focus first on threat levels: intuitively, it seems likely that the probability of a theft attempt in a country such as Japan, for example, with its low threat levels, is fairly low despite the high quality of the material that could be stolen and the relatively modest nature of the security measures in place to protect it, while the probability of a theft attempt in Pakistan seems quite high, given the very high threat there, despite what are believed to be fairly substantial (though not necessarily very high-tech) security measures at its sites.

The second factor is a normalized "theft probability factor," describing the relative likelihood that a theft attempt would be successful, which is based on the difference between the threat level and the security level. This is 1.0 for the extreme case in which the threat is rated 5 and security is only rated 1 (that is, a difference of four points in the ratings); this would be reduced only modestly (to 0.8) when the threat was still three points higher than the security level, but would decline more rapidly as the two ratings neared equality (where the value would be 0.3), eventually dropping to 0.05 at the other extreme, where the security level

[310] I have not used, in this example, a rating scale based on the level of threat the security system at the facility or transport leg being examined was estimated to be able to defend against, as proposed earlier in this chapter, preferring instead to describe an approach based on criteria that could more easily be assessed from outside the country. Governments will full access to relevant classified information may be more able to use a rating system based on the level of adversary capability the security system is estimated to be able to defeat. In any case, such a rating system would be extremely similar to the first approach described in this example, based on estimating the probability that the security system would defeat various levels of threat.

Table 4.13: Attempt and Theft Probability Factors for Different Threat/Security Ratings

Threat Rating	Attempt Probability Factor	Threat/Security Rating Difference	Normalized Theft Prob. Factor
5	0.5	4.0	1
4.5	0.45	3.0	0.8
4	0.4	2.0	0.65
3.5	0.35	1.0	0.45
3	0.3	0.0	0.3
2.5	0.25	-1.0	0.2
2	0.2	-2.0	0.13
1.5	0.15	-3.0	0.08
1	0.1	-4.0	0.05

was four points higher than the threat level. In other words, the probability that a nuclear theft attempt would be successful would be rated as being roughly six times higher if the threat and security ratings were equal than it would be for facilities with the highest possible level of security and the lowest possible level of threat; the probability that a threat would be successful would be somewhat more than three times higher again in the opposite case, where the threat level was as high as possible and the security level was as low as possible. See Table 4.13.

The attempt probability factor and the theft probability factor would be used in the same way as the discount factor described earlier – they would be multiplied by the other factors in the equation in coming to the overall risk rating.

Table 4.14 shows the results of this rating-based approach. Russia and Pakistan are again rated as posing clearly the highest risks, with the unnamed country not far behind. In this approach, however, NRC-regulated HEU-fueled research reactors in the United States are rated as posing higher risks than other U.S. facilities (as opposed to essentially similar risks in the previous approach), despite the moderate quality of the material available to be stolen. Similarly, the material in Uzbekistan is rated as posing higher security risks than the material at non-research-reactor facilities in the United States, despite the relatively low quality of the material there. Moreover, in this approach, Japan and Canada are rated as posing security risks roughly comparable to those for U.S. non-research-reactor facilities (with Canada posing a somewhat lower risk because of the somewhat more extensive security measures there), rather than significantly lower. (This is driven by the fact that in the previous approach, using judgment rather than a fixed rating system to assign the probability of theft attempts, the difference between the theft attempt probability in the United States and that in Japan or Canada was much larger than it is in this approach; even in this approach, lower estimate of the attempt probability factor for countries with a threat rating of 2 would lead to lower estimated risks for Japan and Canada.)

Table 4.14: Country Risk Estimates With a Rating-Based Approach[a]

Country	Threat Level	Sec. Level	Att. Prob.	Theft Prob.	Discount Factor	Risk Rating
Russia	4-5	3	0.45	0.55	1.0	0.25
Pakistan	5	3-4	0.5	0.55	1.0	0.27
United States	3	4-5	0.3	0.16	1.0	0.049
U.S. res. reactors	3	1-2	0.3	0.55	0.4	0.066
Japan	2	2-3	0.2	0.25	1.0	0.050
Canada	2	3	0.2	0.2	1.0	0.040
Uzbekistan	4-5	2-3	0.45	0.65	0.2	0.058
Unnamed Country	3-4	2	0.35	0.55	1.0	0.19

Source: Author's estimates, explained in the text.

In short, as might be expected, where the differences between countries are large (such as the difference in threat levels between Russia and Pakistan and most of the other countries in the example), both methods are quite consistent, but where the balance of different factors is a close call (such as the difference between the low-threat, moderate-security environment in Japan and the moderate-threat, high-security environment for most U.S. facilities), different methods may lead to modestly different results.

To the extent governments and international organizations adopt the basic risk-based approach advocated in this chapter, it would make sense to have several experts give independent ratings to each of the facilities or transport legs being considered, which can then be discussed to arrive at consensus ratings. In either of the approaches described here, a process with multiple different perspectives being considered and debated would likely improve the quality of the outcome.

Using Both Risk and Opportunity to Prioritize Action

Effective policies to reduce the risk of nuclear theft and terrorism must focus not only on where the highest risks lie, but on where the greatest opportunities to reduce those risks lie. One facility may pose a very high risk, but may be located in a country that has flatly refused to cooperate in reducing the risk, while another facility may pose only a moderate risk, but may be located in a country that perceives the danger and is eager to cooperate to reduce the risk. It would be foolish to ignore the opportunity to reduce the danger at the moderate-risk site. But it would also be foolish not to attempt new approaches to convincing the country with the high-risk site of the urgency of action – from raising the issue to higher political levels to offering different sets of approaches and incentives.

In short, risk assessments must be balanced with opportunity assessments, to identify those facilities or transport legs where the largest and fastest reductions in risk can be achieved for any given level of effort available.

Information on which to base assessments of the opportunities at different facilities and transport legs can be drawn from discussions with both on-site officials and national or regional officials – who may have quite different perspectives. An operator of a research reactor, for example, may be absolutely determined to keep the reactor open and may be highly skeptical of converting to LEU fuel, while officials at a national agency that provides the reactor's funding may be facing budget constraints that are already leading them to consider cutting off the reactor's funding and shutting the facility down. A conversation only with the operator might lead to the conclusion that there was little opportunity for progress in eliminating the HEU from that site, while a conversation with the national-level officials might lead to the equally unjustified conclusion that it would be easy to do so; only by understanding the incentives and views of all the relevant stakeholders can a balanced picture of the opportunities be drawn. Often, however, informal conversations by visitors to a site can identify new opportunities quite quickly: in one case, for example, a U.S. expert visiting a small HEU-fueled research reactor was told that the reactor operator would be quite willing to shut down in return for receiving an appropriate radioactive source for seed irradiation, which was more urgently needed than were the missions the reactor was performing.[311]

[311] Personal communication from Jack Edlow, Edlow International, 2003.

5. The Global Nuclear Security System

No engineer in his or her right mind would design a system with hundreds of only loosely controlled nodes, the failure of any one of which could lead to a catastrophic system failure endangering hundreds of thousands of lives and hundreds of billions of dollars in value. Yet, as previous chapters have described, that is a reasonable description of the global system for nuclear security as it exists today. To develop the most effective policies for improving that system and reducing the dangers it poses, it is important to understand the total system and the factors that influence it. This chapter analyzes global nuclear security as a complex, large-scale, integrated, open system (CLIOS)[1] and examines the system's response to past efforts to improve nuclear security. It then examines the record of several policy tools that have been used to try to achieve improvements in nuclear security, in order to make preliminary judgments concerning which policy tools are likely to be most effective in improving nuclear security in the future, under which circumstances. If the qualitative and quantitative arguments presented in Chapters 2 and 3 suggest that improvements in security for nuclear stockpiles could significantly reduce the risk of nuclear terrorism, and the approach presented in Chapter 4 makes it possible to identify the facilities and transport legs where security improvements could make the largest risk-reduction contributions, this chapter asks: how can policy-makers best achieve the needed security improvements for those most-urgent facilities and transport legs?

System Components and Architecture[2]

The fundamental purpose of the global nuclear security system is to prevent hostile or unauthorized acts at nuclear facilities. The most important of these in terms of risks to society as a whole are theft of nuclear weapons or weapons-usable nuclear materials and sabotage resulting in major radiation releases. For many facilities, unauthorized transfer of information designated as national security secrets is also considered to be a high-consequence event the nuclear security system must be designed to prevent (and this aura of secrecy poses very real constraints on international cooperation to improve nuclear security, as discussed below). But acts with far smaller consequences – anti-nuclear protests, petty theft of cash or equipment, mishandling of documents and information, and petty sabotage intended to express frustration rather than to cause a major radioactive release – are the hostile or unauthorized acts that

---

[1] For an introduction of the CLIOS concept, see Joseph M. Sussman, "Toward Engineering Systems as a Discipline" (Cambridge, MA: Massachusetts Institute of Technology, Engineering Systems Division, 6 September 2000; available at http://esd.mit.edu/wps/esd-wp-2000-01.pdf as of 30 December 2006). For a description of a 12-part process for analyzing a CLIOS and designing improvements to it, used in part in this chapter, see Rebecca S. Dodder, Joseph M. Sussman, and Joshua B. McConnell, "The Concept of the 'CLIOS Process': Integrating the Study of Physical and Policy Systems Using Mexico City as an Example" (Cambridge, MA: Massachusetts Institute of Technology, Engineering Systems Division, 5 March 2004; available at http://esd.mit.edu/symposium/pdfs/papers/dodder.pdf as of 30 December 2006).

[2] This section will, in essence, cover the first three steps of the CLIOS process as described in Dodder, Sussman, and McConnell, "The Concept of the 'CLIOS Process'". These include providing an overarching description of the system, including its principal goals; listing its major subsystems; and developing a diagram of the system that includes its major components and their linkages, as an aid to understanding.

actually occur frequently and hence take up a substantial fraction of the time and attention of those involved in the nuclear security system, substantially shaping the system's behavior.

If the system is thought of primarily in terms of the system for preventing theft of nuclear weapons and weapons-usable nuclear materials (the principal subject of this dissertation), then the essential components of the system include:

- Nuclear facilities where nuclear weapons or weapons-usable nuclear materials are located (numbering a few hundred worldwide);
- Institutions that transport nuclear weapons or weapons-usable materials between these facilities;
- The physical equipment used to contribute to security at these facilities, or in transport (from fences and barriers to intrusion detectors and access control systems);
- The personnel at these facilities and transport institutions that play roles important to nuclear security (including not only guards but everyone who handles nuclear weapons and materials, makes decisions on nuclear security matters (including their financing), or is involved in controlling access or deciding on operations that will increase or decrease security risks);
- The firms or institutions that develop, manufacture, sell, install, and maintain the physical equipment used to contribute to nuclear security;
- The firms or institutions that recruit, train, and in some cases manage the personnel involved in nuclear security;
- National regulatory agencies that set nuclear security rules, carry out inspections, and seek to encourage or enforce compliance with those rules;
- National operating agencies that manage and finance government-run nuclear facilities (and that, in some cases, also regulate nuclear security for the facilities under their control);
- National legislatures that pass laws regarding nuclear security and its financing and can exert influence in other ways (such as through holding embarrassing hearings and investigations);
- Central national administrations (such as the Executive Office of the President in the United States, or the prime minister's office in many other countries) that propose laws and budgets for nuclear security and often play a major role in setting the direction for regulatory and operating agencies (whether by appointing their leaders, expressly instructing them to take certain actions, setting their budgets, or other steps);
- International organizations, such as the International Atomic Energy Agency (IAEA) and the United Nations (particularly the Security Council), that make recommendations concerning appropriate approaches to nuclear security (and in some cases provide international peer reviews or help to coordinate international assistance);

- Industry associations that play a role in advising or lobbying national governments on nuclear security, representing the interests of the facilities and transporters that are their members;
- International industry associations (such as the World Nuclear Association) and professional societies (such as the Institute for Nuclear Materials Management), that play a role in sharing experience, ideas, and concerns within countries and across international borders; and
- Media and non-government organizations that provide information to the public and policy-makers on nuclear security matters, sometimes resulting in substantial pressure for change.

The purely technological aspects of the system, from intrusion detectors and access control systems to barriers and vaults, are capable of providing high levels of security at virtually any site (if combined with appropriate numbers of effectively trained, equipped, and motivated guards and other personnel), at a cost that varies depending on the site and the threats it faces. The key problems in this technical-policy system are not with the technology but at the policy levels and in the "human factor" at individual sites and transport legs. The key problems are: (a) how to ensure that policy-makers (from facility managers to national leaders) will in fact make the investments of money, time, and political capital needed to put effective security in place and sustain it, and (b) how to ensure that personnel on the ground will in fact implement security measures effectively.

Figure 5.1 provides a rough sketch of many of these components and how they interact, focusing on the problematic policy levels of the system. To limit the complexity of the figure to a reasonable level, the figure only outlines the components within one particular national system; other governments and their national systems are shown only as unitary components, without internal detail. In some countries, the specifics of the component interactions are different from those shown (which represent roughly the division of responsibilities in the United States). For example, in the United States, nuclear facilities owned by the Department of Energy (DOE) or the Department of Defense (DOD) are also regulated by DOE and by DOD. In other countries there is one nuclear regulator for all facilities, or the division between one regulator and another may relate to military or civilian roles rather than ownership. In Russia, to take a particularly important case, the regulatory agency Rostekhnadzor (the agency into which the former Gosatomnadzor was folded in the 2004 administrative reform) regulates all civilian nuclear activities. But a group within the Ministry of Defense (MOD) regulates all MOD nuclear activities (including both nuclear weapons and nuclear materials, such as the HEU fuel for the nuclear navy) and those activities at the Federal Agency for Atomic Energy (Rosatom, formerly Minatom) that relate to nuclear weapons and their components.

Other aspects of the figure may also vary from one country to another. In some countries, for example, there are no privately-owned nuclear facilities (or no government-owned ones); in other countries, the interests of the media and non-government organizations (and their ability to examine such matters within the constraints of secrecy and government

interference) are so minimal that they should hardly be included as major components of the nuclear security system.

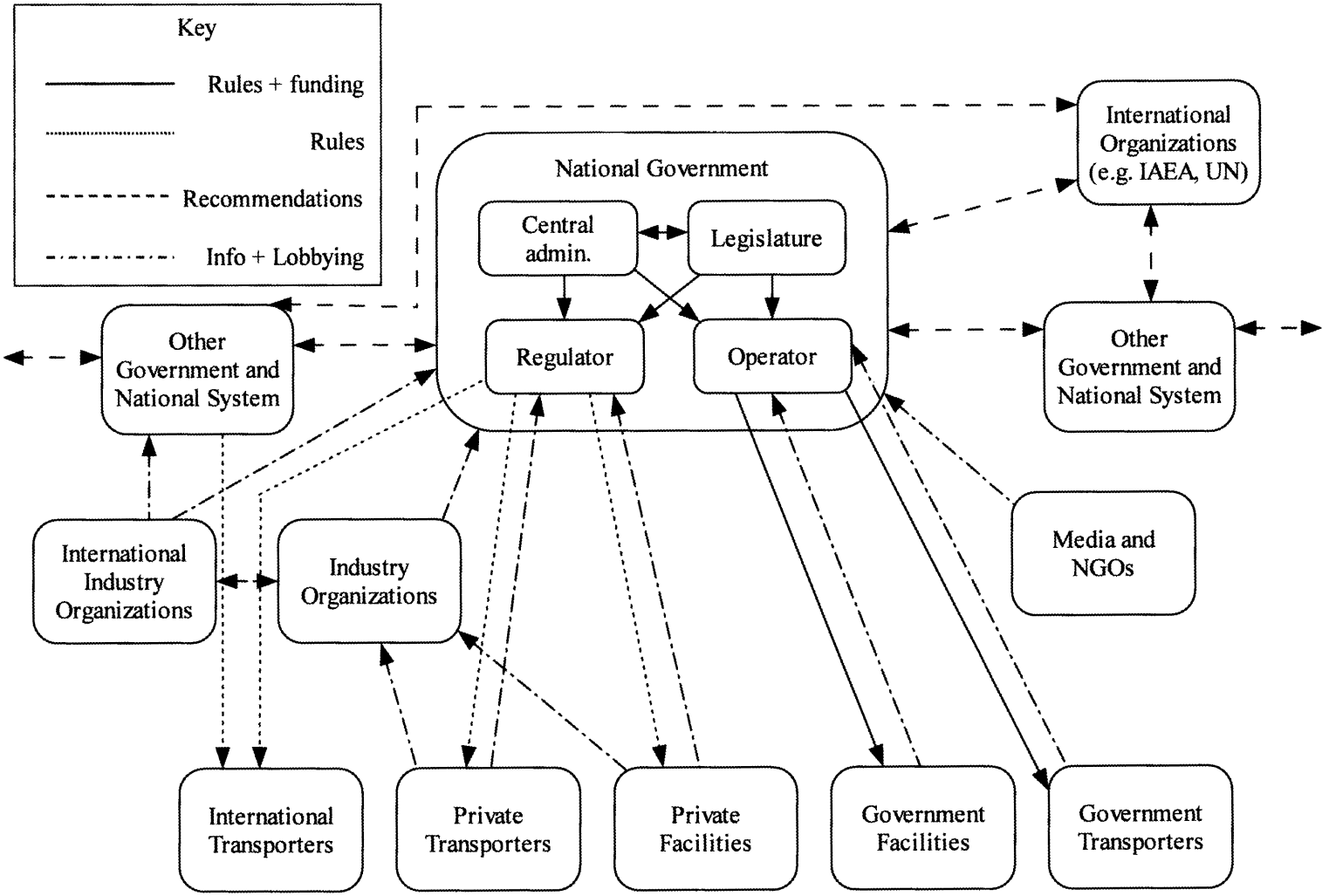
Several aspects of the system shown in Figure 5.1 are worth noting. First, the nation-state is the fundamental unit of organization for nuclear security; each state where these stockpiles exist largely makes its own decisions about what approaches to take to nuclear security, an approach that many states have asserted is a fundamental matter of national sovereignty, as discussed in detail below.[3] To date, the international organizations such as the IAEA and the UN have provided recommendations, but have not asserted the authority to set or enforce binding nuclear security rules; to carry out inspections of nuclear security practices; or even to collect and analyze comprehensive information on nuclear security practices worldwide.[4] Hence, in Figure 5.1, the lines from these international organizations run only to governments that are their member states, not directly to facilities, and represent only recommendations and advice, not setting of rules. Individual governments discuss nuclear security arrangements with each other in a variety of contexts, ranging from bilateral assistance to upgrade material protection, control, and accounting (MPC&A) at individual sites, to requirements by supplier states (especially the United States) that materials and technologies they export must receive adequate protection in the recipient countries – but in most cases these relationships largely take the form of advice and recommendations. When nuclear material is being transported from one country to another, both countries may be involved in setting the nuclear security rules for the trip, as reflected in the rule lines coming from two governments to "international transporters" in Figure 5.1 (though it is also often the case that the supplier country sets these rules essentially unilaterally). Fundamentally, each state is free to determine most of what it will do about nuclear security.

---

[3] For a discussion of this point and of the need to get beyond exclusive national sovereignty in a situation in which poor nuclear security in any country could endanger all other countries, see Lawrence Scheinman, "Transcending Sovereignty in the Management and Control of Nuclear Material," *IAEA Bulletin* 43, no. 4 (2001; available at http://www.iaea.org/Publications/Magazines/Bulletin/Bull434/article7.pdf as of 10 August 2005).

[4] In recent years, international organizations have begun to try to take some steps leading in the general direction of these kinds of activities, but their impact has been modest to date. For example, in April 2004, the United Nations Security Council (UNSC) passed UNSC Resolution 1540, which, *inter alia,* legally required all states with nuclear stockpiles to provide "appropriate effective" security for them. But there has as yet been no international effort to define what the essential elements of an "appropriate effective" nuclear security system are, or to encourage, assist, and pressure states to put those elements in place. Similarly, the IAEA has established a system in which it organizes international peer reviews of a particular state's nuclear security arrangements if that state requests such a review – but there is no current effort to carry out such reviews everywhere, or to collect in-depth information on nuclear security practices in countries that have not been subject to such a review. These points are discussed in more detail in Chapter 5.

Figure 5.1: The Global Nuclear Security System



Second, from the point of view of an individual facility (or nuclear material transporter), the key input on nuclear security comes from the government agencies that set the nuclear security rules and (in the case of government-run facilities) provide the facilities' direction and funding. Thus, in the figure, the flow of influence is primarily vertical, with rules and in some cases funding flowing to the facilities and transporters from the government agencies and information about the difficulties of implementing these rules (and often lobbying to change them) coming back to the government agencies from the facilities and transporters.

It appears that on nuclear security matters, there is remarkably little horizontal flow of information – between facilities, or between governments – about issues they are facing or incidents that have taken place. (Figure 5.1 includes no links at all between facilities, which may overstate the case somewhat, but apparently not by a great deal.) In a Moscow roundtable with Russian participants in the U.S.-Russian MPC&A program in October 1999, for example, it was clear that the representatives from different sites had not previously had a chance to discuss the problems they were having in cooperating with the United States and were extremely interested in the approaches other sites had taken in the face of similar problems.[5] Similarly, in discussions with Russian experts at several sites in 2005, none of them were aware of the incident at Sarov in which a Russian businessman had been offering $750,000 for stolen weapon-grade plutonium – surely an important event in considering the likely magnitude of the insider threat.[6] In the United States, the situation appears to be only modestly different – facilities have few regular channels for discussing their nuclear security issues with each other, rather than with headquarters.

In the United States, and to varying degrees in other countries, other actors play substantial roles in the system as well. Industry organizations actively seek approaches to nuclear security that they see as serving industry's interests and therefore provide information and lobbying to regulators, central governments, and legislatures. International industry organizations, such as the World Nuclear Association, play a more modest role in this respect. The press and non-government organizations (NGOs) outside the nuclear industry often provide information (and lobbying, in the case of NGOs) to the same parties in government, often swaying the balance toward greater concern and more stringent regulation.

System Properties and Behavior[7]

System Drivers: Incidents and Investigations

Long-time observers make the point that the nuclear security system in the United States and worldwide is "incident-driven." A major incident – such as a large loss of nuclear

---

[5] Workshop on MPC&A, sponsored by the Russian-American Nuclear Security Advisory Council, 1999.
[6] Interviews, May and July 2005.
[7] For economy of space, this chapter does not pursue a detailed description and characterization of each component and linkage in the system, the fourth step of the CLIOS process as described by Dodder, Sussman, and McConnell, preferring to leave it with the summary description just provided. The section that follows, describing the behavior of the system, corresponds to the fifth step of the CLIOS process. See Dodder, Sussman, and McConnell, "The Concept of the 'CLIOS Process'".

material or a terrorist attack – highlights the dangers and convinces policy-makers and regulators that more stringent nuclear security measures are needed. For a period, there is a great deal of spending and activity to upgrade security; then, as the incident recedes into the past, complacency begins to set in, and budgets begin to be reduced again.[8] Examples include:

- the substantial improvements in accounting for nuclear materials introduced after the apparent loss of nearly 200 kilograms of HEU from the Nuclear Materials and Equipment Corporation (NUMEC) in 1965;[9]
- the significant changes in security rules and organizations (including the establishment of the National Nuclear Security Administration) following the allegations of Chinese espionage in the 1990s; and
- the major changes in approaches to nuclear security in the United States and many other countries around the world following the 9/11 attacks.

The events that laid the foundation for modern approaches to physical protection of nuclear sites in the United States and around the world, from the late 1960s to the mid-1970s, are also, in part, a reflection of this incident-driven pattern. Concerns provoked by the outbreak of international terrorism (and domestic hijackings) in the years following the 1967 Arab-Israeli war, culminating in the 1972 terrorist attack on the Munich Olympics, contributed substantially to major changes in U.S. physical protection rules and practices (including the establishment of the first real systems-engineering approaches to nuclear security, beginning in the early 1970s); the development of the first IAEA recommendations on physical protection; the imposition of U.S. requirements for adequate physical protection of U.S.-supplied nuclear material in other countries; and the U.S. initiative to include physical protection requirements in the guidelines of the Nuclear Suppliers Group.[10] But the string of

---

[8] Dennis Mangan, Sandia National Laboratory, remarks to the workshop on "Comparative Analysis of Approaches to Protection of Nuclear Materials," Stanford University, 28-30 July 1997. Mangan was one of the first employees of the physical protection group at Sandia National Laboratories when it was established in the early 1970s and has been working in the field ever since.

[9] The apparent HEU loss at NUMEC from startup to October 31 1965 was 178 kilograms. See W. Altman, J. Hockert, and E. Quinn, *A Safeguards Case Study of the Nuclear Materials and Equipment Corporation Uranium Processing Plant: Apollo, Pennsylvania*, vol. NUREG-0627 (Washington, DC.: U.S. Nuclear Regulatory Commission, 1979), p. 18. Some of this was losses to waste, but some appeared difficult to explain. There were a series of investigations of the possibility that facility head Zalman Shapiro, who had close ties to leading Israeli defense and intelligence officials, had provided the missing HEU to Israel, but nothing was ever proved. A substantial amount of HEU was found when the facility was decommissioned years later, suggesting the possibility that nothing was ever stolen from the facility, as Shapiro had argued all along. See Seymour Hersh, *The Samson Option: Israel's Nuclear Arsenal and American Foreign Policy* (New York: Random House, 1991), p. 257. The impact of this incident on new material accounting rules, reviews of physical protection procedures, and the establishment of a nuclear safeguards research and development program at Los Alamos is mentioned in William J. Desmond, Neil R. Zack, and James W. Tape, "The First Fifty Years: A Review of the Department of Energy Domestic Safeguards and Security Program," *Journal of Nuclear Materials Management* 26, no. 2 (Spring 1998). See also discussion in J. Samuel Walker, "Regulating against Nuclear Terrorism: The Domestic Safeguards Issue, 1970-1979," *Technology and Culture* 42, no. 1 (January 2001).

[10] Mangan's 1997 remarks emphasized the importance of Munich, as did J.D. Williams (another of the first employees of the Sandia physical protection group, who continued in the field until his death), in an interview in

terrorist incidents that occurred in this period were not the sole cause of these changes in nuclear security approaches. Other trends and events that contributed to the public and government concerns that led to these changes included:

- a rapid expansion of the nuclear industry, with a planned reliance on reprocessing and recycling of plutonium, creating expectations that tens or hundreds of tons of separated plutonium would soon be in circulation among scores of facilities every year;
- the rise of general public concern over nuclear energy (of which concerns over security were only one part) and the establishment of well-informed anti-nuclear organizations who were able to channel that concern into pressure for more stringent regulations;
- the experiences of Vietnam and other events of the 1960s and early 1970s, which undermined public confidence in government and industry assurances that all appropriate measures to manage complex technologies were already being taken;
- the critiques of insiders within the nuclear establishment who raised major concerns over the adequacy of nuclear security arrangements (most notably Theodore B. Taylor, profiled in John McPhee's classic book from the period, *The Curve of Binding Energy*); and
- the Indian nuclear test in 1974, which heightened fears of nuclear proliferation in general and concerning the availability of separated plutonium in ostensibly civilian nuclear programs in particular.

These incidents and trends led a dramatic increase in public concern over nuclear security in the 1970s, which was the first time when the danger of nuclear theft and terrorism was publicly debated. But as the nuclear security system was structured (and even more as the structure has evolved since then) such major shifts in the public view were only weakly coupled to comparably large changes in approaches to nuclear security. At the time, the nuclear industry argued that these public concerns were overblown, and while significant new nuclear security rules were imposed, the industry was successful in limiting their scope and cost. By the 1980s much of the public concern over nuclear security (and the resulting pressure for tighter nuclear security rules) had dissipated: the Three Mile Island and Chernobyl accidents focused public concern over nuclear energy on safety, rather than security, and made clear that the previously projected rapid growth of nuclear energy was not going to happen; plans for a plutonium economy fizzled, except in a few countries; with the escalating U.S.-Soviet competition, nuclear fears centered on nuclear war rather than terrorism; security regulations were already in place that regulators and the industry argued were adequate; and there were few dramatic incidents to drive public concern. In short, long-

---

September 2002. Major revisions of U.S. physical protection rules were issued in 1970 and 1973; the first IAEA recommendations on physical protection, known as the "gray book" was published in 1972; a physical protection research and development program was established at Sandia in 1973, following Munich; also after Munich, major upgrades were undertaken in protection for U.S. nuclear weapons; the U.S. imposition of physical protection requirements for U.S. nuclear exports evolved over roughly 1972-1975; the Nuclear Suppliers Group meetings that worked out the initial guidelines, including the physical protection requirements, were in 1975. See, for example, Desmond, Zack, and Tape, "The First 50 Years"; Walker, "Regulating against Nuclear Terrorism"; Victor K. McElheney, "U.S. Adding to Safeguards in Tactical Nuclear Arms," *New York Times*, 18 December 1973.

term changes in public opinion do occur, and do have an effect on the nuclear security system, but the coupling is weak and it is rare for public opinion to focus on nuclear security and terrorism for long.[11]

Major investigations that produce embarrassing findings – whether internal to the executive branch, initiated by the legislature, or carried out by the press or non-government organizations – can also be system drivers, acting in much the same way as major terrorist incidents. (In the case of external investigations, however, there is a greater tendency to resist the resulting pressure for action than in the case of a major terrorist incident, as the investigation itself and the calls for action resulting from it can be dismissed as the work of anti-nuclear critics.) The most prominent example here (but by no means the only one) is the series of congressional investigations of security at DOE nuclear sites led by Rep. John Dingell (D-MI) in the 1970s and 1980s, which created immense pressure for action to upgrade security at DOE.[12]

Figure 5.2 illustrates this basic trend.[13] As noted in the figure, an organization cannot focus exclusively on protection or it will go bankrupt; and it cannot ignore protection or it will face a catastrophe. Between these extremes, the figure shows a hypothetical organization moving through what Reason calls the "production-protection space." It begins with somewhat more emphasis on protection than production; as no incidents occur, efforts are made to cut back on protection costs, and the organization drifts toward increasing emphasis on production. A small incident occurs and pushes the organization to focus more on protection again, but this is again followed by drift toward a production emphasis, until a larger incident occurs. That then leads to renewed commitment to protection. But after a prolonged period without incidents, the "unrocked boat" drifts so far away from protection that a catastrophe occurs. While this was intended as a description of the behavior of a single organization, it is a reasonable first approximation to the behavior of the entire nuclear security system. In a similar vein, the U.S. General Accounting Office has described airline security efforts over the years as "a cycle of limited action," in which the absence of a "major

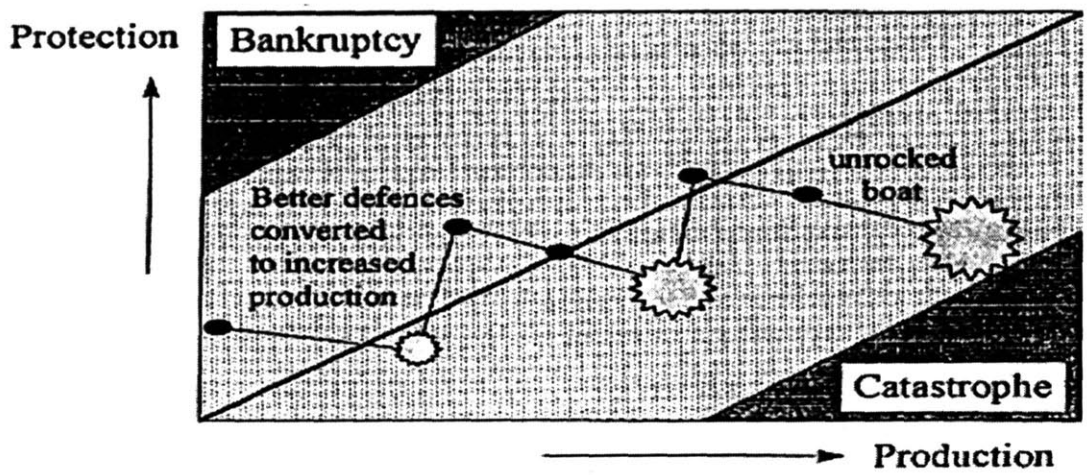
---

[11] For a discussion of how politics and public opinion have shaped government oversight and regulation of nuclear energy in the United States more generally, see Robert J. Duffy, *Nuclear Politics in America: A History and Theory of Government Regulation* (Lawrence, Kans.: University Press of Kansas, 1997).

[12] See, for example, Committee on Energy and Commerce, *Nuclear Weapons Facilities: Adequacy of Safeguards and Security at Department of Energy Nuclear Weapons Production Facilities*, U.S. Congress, House of Representatives, 99th Congress, 2nd Session, 6 March 1986. For examples of investigations by non-government organizations that created substantial pressure for change, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Security at Risk* (Washington, D.C.: POGO, 2001; available at http://www.pogo.org/p/environment/eo-011003-nuclear.html as of 4 December 2006); Project on Government Oversight, *Nuclear Power Plant Security: Voices from inside the Fences* (Washington D.C.: POGO, 2002; available at http://www.pogo.org/p/environment/eo-020901-nukepower.html as of 2 January 2007).

[13] Figure is from James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, U.K.: Ashgate, 1997), p. 5. The figure originally illustrated a discussion of safety, but is equally applicable to security.

Figure 5.2: An Incident-Driven Passage Through the Production-Protection Space



Source: James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, U.K: Ashgate, 1997), p. 5.

security incident...could breed an attitude of complacency...Improving security in such an environment is more challenging and difficult."[14]

Officials charged with appropriating funds for nuclear security and drawing the protection-production balance – from cabinet ministers to facility managers – often find it difficult to judge, when security officials request additional funds for security improvements, whether those additional resources are really needed. Security can *always* be improved, and security officials are often seen as professional paranoids always demanding more, yet the minister or manager does not want to spend his organization into bankruptcy. Institutional mechanisms for determining whether security at a given site is adequate to defend against a particular specified threat, with results that are clear and demonstrable to policymakers, are crucial to help policy-makers navigate the protection-production space. One such mechanism that has been used extensively in the United States is performance testing – observing how the security system does in realistic tests of the ability of outsiders to shoot their way in, or of insiders to smuggle out nuclear material or conduct a successful sabotage.[15]

---

[14] Quoted in Max H. Bazerman and Michael D. Watkins, *Predictable Surprises: The Disasters You Should Have Seen Coming and How to Prevent Them* (Cambridge, Mass.: Harvard Business School Publishing, 2004), pp. 17-35.

[15] For discussions of performance testing and its importance (along with its weaknesses), see, for example, Oleg Bukharin, "Physical Protection Performance Testing: Assessing U.S. NRC Experience," *Journal of Nuclear Materials Management* 28, no. 4 (Summer 2000); Oleg Bukharin, Matthew Bunn, and Kenneth N. Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union* (Washington, D.C.: Russian American Nuclear Security Advisory Council, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mpca2000.pdf as of 2 January 2007).

System Constraints I: Complacency, Structural Disincentives, and Policy Resistance

Of course, when an incident or investigation occurs, the global nuclear security system does not immediately shift to a new state reflecting what a classical rational actor might judge was an appropriate response. Rather, the impulse is mediated through a range of organizations, many of which tend to be reluctant to change established policies – and many of which have only limited ability to cause other actors in the system to change their policies, even should they wish to do so.

Complacency, in particular, is a major constraint on the system's ability to respond appropriately to new conditions. In nuclear agencies and facilities worldwide, many officials believe that a major outsider attack on a nuclear facility (either for theft or sabotage) in their country is so unlikely as to be essentially implausible; that similar insider actions are also implausible; that it would be so difficult for terrorists to make a nuclear bomb, even if they got the nuclear material, that this danger can be effectively dismissed; and that existing nuclear security measures are sufficient, or even excessive.[16]

The problem of complacency and how to counter it permeates the nuclear security system. A government minister who is complacent about the threat is unlikely to impose more stringent nuclear security rules or allocate additional funds to nuclear security. A facility manager who is complacent about the threat is likely to put nuclear security low on his or her list of priorities for allocation of money and management attention – an attitude that will be quickly communicated to all of the facility's staff, whether it is ever publicly stated or not. Guards and other security-relevant personnel who are complacent about the threat are unlikely to go the extra mile to check out every suspicious event and are likely to cut corners on nuclear security rules. James Reason's remark about safety is equally applicable to security: the key to maintaining an adequate focus on protection within an organization is "not forgetting to be afraid."[17]

There are good reasons for this complacency, making these views easy to defend and quite difficult to change. For example, although there have been a variety of incidents of different types over the years, there has never been a major terrorist attack on an operating nuclear facility that was intended either to steal nuclear material or to cause a major radiological release. Similarly, there is no conclusive evidence that there has ever been a successful insider theft of enough material for a nuclear bomb, or an incident of insider sabotage that was really intended to cause a major radioactive release. As discussed in Chapter 2, there is as yet no convincing evidence that terrorist groups have in fact pulled together the needed capabilities or made much progress in getting hold of stolen plutonium or HEU to build a bomb from (let alone a stolen nuclear weapon). In all likelihood, 99% of the

---

[16] For a discussion of these and other "myths" that cause many to downplay the danger of nuclear terrorism, with quotes from leading officials expressing these views, see Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007).

[17] Reason, *Managing the Risks of Organizational Accidents*, p. 195.

guards and other security-relevant personnel at nuclear facilities around the world will never experience a real attempt to steal nuclear material or cause a radioactive release at their facility during their entire careers. Ensuring that nuclear organizations and their personnel do not become complacent about the risk of events that never occur is one of the most difficult policy problems facing the global nuclear security system.

The alert reader, however, will notice that most of the sentences in the preceding paragraph include a variety of caveats. Without those caveats, they would not be true. There *have* been, for example, numerous terrorist attacks on nuclear facilities over the years, though none of these were clearly intended to steal nuclear weapons or materials or cause a major radioactive release.[18] Most appear to have been intended to protest nuclear energy or stop the construction of a particular plant (as was the case with the large number of Basque separatist attacks on nuclear facilities in the 1970s and 1980s in Spain and the firing of a rocket-propelled grenade – a commonly available terrorist weapon that facilities regulated by the U.S. Nuclear Regulatory Commission (NRC) are still not required to defend against – at the French Superphénix plant in 1982). Many nuclear officials dismiss the likelihood of a terrorist attack on a guarded nuclear facility, arguing that terrorists will prefer to strike soft, undefended targets. But there has in fact been a case of a group of heavily armed terrorists attacking a military base with nuclear weapons (the 1977 attack on the U.S. base at Giessen, in Germany, by the Baader-Meinhof gang);[19] there has also been a case in which a group of 15 armed terrorists attacked a nuclear facility, overwhelmed the five guards on duty at the time, and seized control of the facility (this was the 1973 attack on the Atucha Atomic Power Station in Argentina, which was not yet operating at the time).[20] Similarly, there has been a case of an attacker hijacking a civilian passenger aircraft and threatening to crash it into a nuclear facility, something often dismissed as extremely unlikely in the months after 9/11 (this was the plane that hijackers threatened to crash into the Oak Ridge National Laboratory in 1972).[21]

---

[18] See, for example Konrad Kellen, "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists," in *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Cambridge, Mass.: Lexington Books for the Nuclear Control Institute, 1987). For a partial update, see William Robert Johnston, "Nuclear Terrorism Incidents" (28 September 2003; available at http://www.johnstonsarchive.net/nuclear/wrjp1855.html as of 5 January 2007).

[19] A somewhat exaggerated account of this attack is provided in the opening chapter in Andrew Cockburn and Leslie Cockburn, *One-Point Safe* (New York: Anchor Books/Doubleday, 1997). In an interview, the commander of the base at the time (who appears to have been a major source for the Cockburns' description of the incident), argued that the terrorists who attacked were *not* attempting to seize the nuclear weapons at the base (which would have required more firepower than they attacked with) and may have been unaware that there were any nuclear weapons present at the time; in his view, the weapons at the base were never in any danger. Interview with Maj. Gen. William Burns (U.S. Army, Ret.), August 2002.

[20] For a discussion of this episode, see Kellen, "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists." The terrorists seized 11 guns from security posts at the site, painted revolutionary slogans on the walls, and then departed. As they were leaving police responders arrived, and there was a shoot-out that left two policemen wounded before the terrorists disappeared into the jungle. As of 1987, they had not been identified or apprehended.

[21] Malcolm Gladwell, "Safety in the Skies: How Far Can Airline Security Go?" *The New Yorker* (1 October 2001; available at http://www.newyorker.com/fact/content/articles/011001fa_FACT as of 24 August 2005).

While there are no successful confirmed incidents of theft of enough nuclear material for a bomb, there are numerous confirmed incidents of theft of smaller quantities of plutonium or HEU. As discussed in Chapter 3, the CIA has assessed that undetected thefts have probably occurred. Moreover, Russian officials have confirmed that in 1998, at a major nuclear facility in the Chelyabinsk region, there was an insider conspiracy that attempted to steal 18.5 kilograms of HEU – potentially enough for a bomb, depending on the enrichment.[22] Finally, as discussed in Chapter 2, there is ample evidence that terrorists are seeking nuclear weapons, and a range of government studies have convincingly demonstrated that constructing a crude nuclear bomb is well within the plausible technical capabilities of a well-organized terrorist group. If incidents such as these were widely known and regularly discussed in the nuclear industry, complacent attitudes might begin to change; that they are not well known among officials deciding on the levels of effort to devote to nuclear security has to do in part with the pervasive secrecy surrounding nuclear security matters, another important system constraint discussed below.

Because stringent nuclear security measures are expensive, nuclear industry officials have strong incentives to maintain complacency and convince themselves that additional security measures are not needed. The tendency to downplay risks that would be expensive or inconvenient to address is only one example of the human tendency to believe what it is in our interest to believe, present in essentially every human industry and activity; who among us has not, at some point in our lives, put off practicing what we would do in the event of a fire in our home, reasoning (contrary to the available evidence) that this risk is so low as not to be worth bothering with? Cognitive dissonance – which often leads people to focus on those facts that support what they already believe, while ignoring facts that challenge those views – plays a very critical role in maintaining such complacency. People in the nuclear industry, like people everywhere else, tend to convince themselves that the ways they are doing things now are appropriate and reasonable, finding reasons to dismiss evidence to the contrary; no one is easily able to accept that the standard practices they and their friends and colleagues have been following may pose a serious danger to the world. Hence, nuclear security officials tend to press for less stringent nuclear security rules, in the sincere belief that their recommendations are justified. This is but one example of the common saying "where you stand is where you sit."

Because of people's ability to focus on confirming evidence and ignore contrary evidence, the perception that the security measures in place are already sufficient does not appear to be closely related to what those security measures actually are; that view was widespread in the nuclear industry even when only the most minimal security measures, which would now be agreed by all to be grossly inadequate, were in fact in place. In 1973,

---

[22] It was the Federal Security Service that first announced that it had foiled an insider conspiracy to steal 18.5 kilograms of nuclear material from a major facility in Chelyabinsk. A MINATOM official later provided somewhat more detail in an interview. See Yevgeniy Tkachenko, "FSB Agents Prevent Theft of Nuclear Materials," *ITAR-TASS*, 18 December 1998; "Interview: Victor Yerastov: Minatom Has All Conditions for Providing Safety and Security of Nuclear Material," *Yaderny Kontrol Digest* 5, no. 1 (Winter 2000). That the material concerned was HEU was confirmed by a MINATOM official in an interview with the author, June 2000.

for example, representatives of the U.S. nuclear industry reacted sharply against what they called a "regulatory flash flood" of new security rules, specifically arguing, for example, that there was no need for the then-new requirements that plutonium reprocessing plants and transports of plutonium and HEU have armed guards.[23]

Security rules that do not seem to make sense are one important source of complacency in nuclear organizations (as in any organization). Virtually everyone who has ever worked in any large organization has had the experience of being confronted with rules that seemed to make no sense and which most people violated. When security rules are put in place that seem to those who have to implement them to be burdensome and costly without providing any real security benefit, they will tend to violate those rules. If this is a common situation, then each employee will be making frequent judgments as to which rules to follow and which rules to ignore, and a culture of frequent violation of security rules will be the inevitable result. People will tend to do what they believe it is important to do;[24] if security rules are set and employees are trained so that all security-relevant employees understand what the rules are and come to believe that they are important, the rules will be followed. Minimizing "stupid rules" is a key part of building an effective security culture.

Nuclear security is only one of a large class of problems in which complacency and reluctance to change past practices are reinforced by large structural disincentives that deter participants from addressing the problem. The costs of action are certain and present, while the benefits of action are highly uncertain and accrue at some unknown point in the future. Affected constituencies will notice the costs of action immediately, but when a disaster does not occur, may not believe that this is the result of the action taken. In many cases the costs of action are borne by a small minority (which therefore has very strong incentives to oppose action) and the benefits are spread thinly over the general public (which therefore has little incentive for focused support for action). Max Bazerman and Michael Watkins have recently categorized this class of problems as "predictable surprises" – cases in which most organizations fail to act to prevent disasters they should have seen coming.[25] Nuclear terrorism is a classic predictable surprise, incorporating essentially all the causes of such surprises Bazerman and Watkins identify. Bazerman and Watkins outline a wide range of both cognitive and organizational problems that make it difficult to address predictable surprises. In the case of nuclear security, the structural disincentives to action are substantial, as every dollar a senior official devotes to nuclear security is a dollar not devoted to other activities that may well be more politically popular; every dollar a facility manager devotes to nuclear security is a dollar not devoted to activities that would generate revenue; and every

---

[23] See, for example, the magazine *Nuclear Industry,* issues of February 1973, March 1973, and May 1973, quoted in Walker, "Regulating against Nuclear Terrorism," p. 116.

[24] In one intriguing study, for example, researchers found that a perception that compliance with a rule was important reduced the probability of non-compliance to very low levels even if the chances that violation would be detected were seen as "low to moderate." By contrast, if there was a personal benefit in violating the rule, the chances of violation were several times higher even if the perceived likelihood of detection was moderate to high. See Reason, *Managing the Risks of Organizational Accidents*, p. 145.

[25] Bazerman and Watkins, *Predictable Surprises*.

hour that a worker at a facility devotes to following nuclear security rules is an hour not devoted to activities more likely to result in a raise or a promotion.[26]

The complacency and structural disincentives to action just described often motivate nuclear managers to resist efforts to tighten nuclear security rules and to seek exemptions or other cost-saving measures to ameliorate the effects of the rules already in place. These efforts typically take the form of lobbying and providing advice to the institutions which set and enforce these rules, arguing for looser rules, interpretations of the rules that would allow lower-cost approaches to their implementation, and the like. On an issue like nuclear security, such industry advice and lobbying can be extremely influential, for reasons discussed in more detail below.

Hence, the global nuclear security system exhibits substantial policy resistance – the tendency of a system to resist policy initiatives and to drift back toward the system state that existed prior to the initiative.[27] In essence, outside advocates for increased nuclear security (who typically are not among those who have to pay for it) and the nuclear industry have competing goals (increased nuclear security in one case, minimized costs in the other), and the effect of advocates working to achieve these goals is that the overall system will tend to come into balance between them. A redoubled effort by one faction to shift the system balance in its direction will result in redoubled efforts by the opposing faction to drag the system back the other way.

Of course, participants in the nuclear industry are at the same time members of the broader society and will reflect broader societal concerns as well. If a major incident causes a broad consensus to develop that increased security measures are needed – as occurred with the 9/11 attacks – the industry will generally support some new security measures, while at the same time seeking to ensure that they do not unduly undermine the industry's interests. In the United States after 9/11, for example, the Nuclear Energy Institute (NEI), the lobbying arm of the nuclear industry, supported more stringent nuclear security rules, while at the same time launching a major campaign to convince the NRC and the public that NRC-regulated facilities were already so secure that only modest further improvements were necessary.[28]

---

[26] Matthew Bunn, "Incentives for Nuclear Security," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

[27] For a discussion of policy resistance in the context of the dynamics of complex policy-technical systems (which may have been the article that first introduced the term "policy resistance" in this context) see Donella H Meadows, "Whole Earth Models and Systems," *CoEvolution Quarterly* (Summer 1982; available at http://www.oss.net/dynamaster/file_archive/040324/48c97c243f534eee32d379e69b039289/WER-INFO-73.pdf as of 15 August 2005), pp. 98-108. See also John Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World* (Irwin: McGraw-Hill, 2000), pp. 5-14.

[28] The Nuclear Energy Institute's argument that U.S. facilities have greatly improved security since 9/11 and are now highly secure, without requiring further improvements, is summarized in Nuclear Energy Institute, "Fact Sheet: Nuclear Power Plant Security" (Washington, D.C.: NEI, March 2005; available at http://www.nei.org/index.asp?catnum=3&catid=48 as of 18 August 2005). For a detailed discussion of the NRC's approach to improving security since 9/11 and the role that the nuclear industry has played in it, see Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, *Nuclear Security: Has the NRC Strengthened Facility Standards since 9/11?* U.S. House of Representatives,

Nuclear Regulation Within the Overall System

Effective nuclear security rules that are effectively enforced are critical to the maintenance of appropriate nuclear security programs, because managers will generally avoid making expensive investments in security, rather than in other activities that could bring in revenue, unless they have to. Hence, the nuclear regulatory agencies are key points of policy leverage in the overall nuclear security system.

But in many cases, the regulatory agencies charged with setting and enforcing nuclear security rules are in a very difficult position within the system. Many regulatory agencies are a good fit for James Q. Wilson's model of agencies created in response to "entrepreneurial" politics: some perceived crisis makes it possible for policy entrepreneurs to create an agency to "rein in" a particular industry, even though the industry is initially hostile. But the costs of the regulation are focused in one industry, giving it strong incentives to devote substantial efforts to influencing the regulatory agency to moderate its rules, while the benefits of stringent rules are broadly distributed across society as a whole, giving the general public only modest incentives to support stringent rules. Hence, after the initial crisis is past and interest flags, the agency "may find itself confronting an environment where much of the information it needs and many of the political resources to which it must respond will be in the hands of an interest fundamentally hostile to its purposes."[29] Agencies in this position, Wilson warns, are in danger of "capture" – of coming to serve the interests of the industry they were intended to control – though this is not inevitable.

The nuclear industry is often in a position to be very persuasive with nuclear regulatory bodies in the security area, for several reasons. In most cases, the regulatory agencies are substantially smaller than the industries and agencies they are supposed to control and have less expertise and political power. Most of the relevant technical expertise needed to address the issues persuasively resides in the industry itself. Most of the relevant information is classified, limiting the effectiveness of outside parties who might disagree with industry's view; industry has access to the relevant information about its security practices and the specifics of the security rules it faces, and outside critics usually do not. The nuclear regulatory agencies not only get much of their information and perspectives from the industry, but they typically draw most of their personnel from the industry – and many of these personnel plan on returning to the industry after their stint at the regulatory agency. Under these circumstances, it is not surprising that the predominant views and approaches held in the regulatory agencies would in many cases come to closely reflect the views and approaches that are dominant in the industry they regulate.

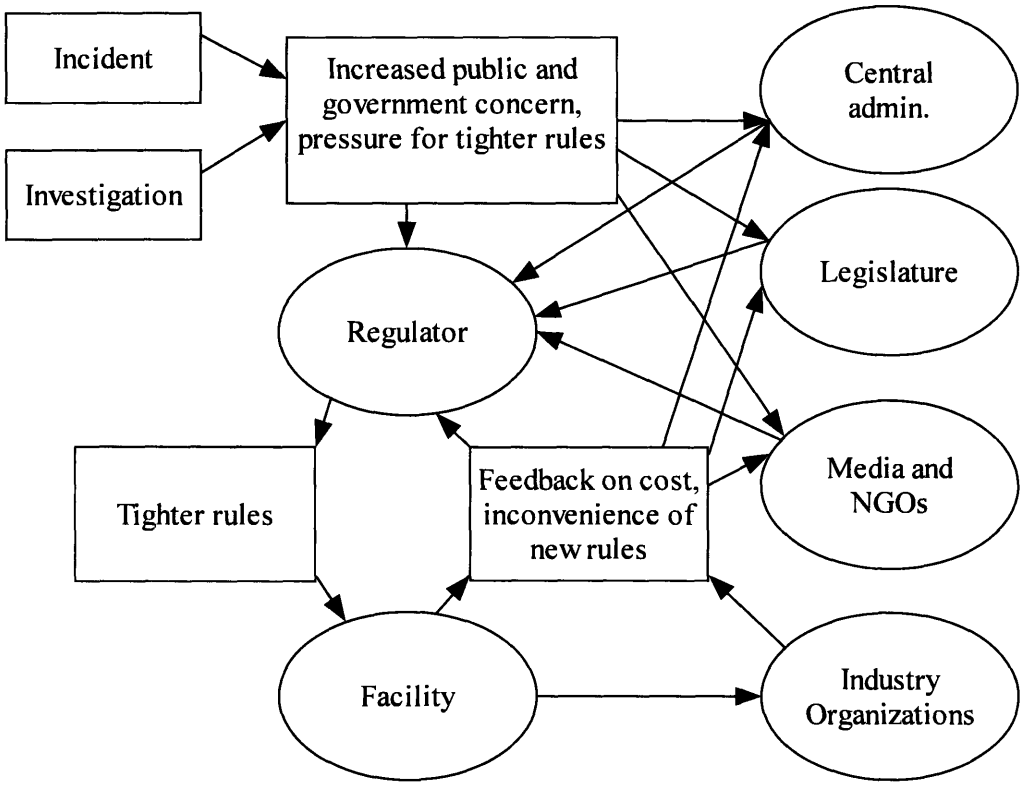
Moreover, the regulatory agencies are often under considerable pressure from central governments and legislatures not to impose rules that would be unduly costly and thereby potentially undermine the future of nuclear energy. While these regulatory agencies are, in

---

109th Congress, 2nd Session, 4 April 2006 (available at http://reform.house.gov/NSETIR/Hearings/EventSingle.aspx?EventID=41937 as of 6 May 2006).

[29] James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It*, 2nd ed. (New York: Basic Books, 2000), p. 78. See also "The Regulator's Unhappy Lot," in Reason, *Managing the Risks of Organizational Accidents*.

Figure 5.3: Influences at the Regulator and Facility Level



some cases, simultaneously under pressure from non-government organizations and others to fix perceived nuclear security weaknesses, the advocates of more stringent rules usually have much less expertise and power to bring to bear on the problem than the industry does. Given these constraints and pressures, it is remarkable that nuclear regulatory agencies in some countries have been as effective as they have.[30]

Figure 5.3 illustrates some of the inputs and feedbacks operating between a regulatory agency and the facilities it regulates. A major incident or investigation leads to public and government concern and pressure for tighter nuclear security rules – pressure the officials of the regulatory agency feel themselves after the incident or investigation, but pressure that also comes from central governments, legislatures, the media, and NGOs. After a period of review and input from both industry and other parties, the regulatory agency revises its rules. The facilities then provide feedback to the agency on the costs and inconveniences caused by the new rules and in many cases may suggest modifications or approaches to implementing the rules that could save money or reduce the inconvenience of following the new rules. Industry organizations representing the interests of the facilities help carry the messages the facilities

[30] For a discussion of interactions between the U.S. Nuclear Regulatory Commission, the nuclear industry, and NGOs advocating tighter nuclear security in the United States in the years after the 9/11 attacks, see *Nuclear Security: Has the NRC Strengthened Facility Standards since 9/11?*

are sending, to the regulator and to others who might pressure the regulator (such as the legislature and the central government). Outside critics, at the same time, may press for even tighter rules, but are likely to have less influence than the more powerful and better-informed industry. This sets up a classic cycle of tugging and hauling – but one in which the industry is generally better positioned than outside critics are. Thus, until the next driving event, the general trend (though often a very slow one) is likely to be toward relaxation rather than further ratcheting up of the rules.

System Time Lags, Delays, and Lock-In

Time lags and delays are an important property of the nuclear security system. The delays imposed by the *technical* components of the system are modest. In principle, for example, with sufficient political agreement, nuclear material can be airlifted out of a vulnerable site in days or weeks. In many cases in U.S.-Russian cooperation, very significant initial "rapid" security upgrades – fixing holes in fences, installing equipment to detect plutonium or HEU being removed, bricking over windows, placing material in steel cages – have been accomplished in six months or less from the start of work, and "comprehensive" security and accounting upgrades, involving installation of an entire suite of modern nuclear security and accounting equipment (with associated training) have been completed in 18 months.[31]

The typical delays in the *policy* components of the system are usually substantially longer – though if political actors at a high enough level push hard enough, such delays can be dramatically reduced. In most cases, however, such high-level pressure for immediate action, sweeping aside the usual bureaucratic processes, is absent or modest; in such cases, rules take years to write, more years to implement, and the time from policy initiative to result can be very long. This is a problem, because the galvanizing effect of the incident that originally drove a decision to require more stringent rules tends to fade at a rate comparable to the rate at which the new rules are developed and implemented. In the United States after the 9/11 attacks, for example, it took the NRC more than 19 months (and DOE 20 months) to issue new rules requiring facilities to be able to defend against larger and more capable threats.[32] DOE then issued a further revision in the fall of 2004 (three years after the 9/11 attacks); DOE

---

[31] U.S. Department of Energy, *FY 2006 Congressional Budget Request: National Nuclear Security Administration--Defense Nuclear Nonproliferation*, vol. 1, DOE/ME-0046 (Washington, D.C.: DOE, 2005; available at http://www.cfo.doe.gov/budget/06budget/Content/Volumes/Vol_1_NNSA.pdf as of 27 February 2006), p. 486. Even without major upgrade initiatives of this kind, the technical turnover time of the nuclear security system is much shorter than that, say, of typical large energy facilities: rather than being replaced only every 40-50 years, most of the components of a nuclear security and accounting system are designed to be replaced roughly every 10 years.

[32] NRC issued its new DBT on April 29, 2003, though it had issued a number of previous advisories and orders. See U.S. Congress, General Accounting Office, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: GAO, 2003; available at http://www.gao.gov/new.items/d03752.pdf as of 15 August 2005). DOE's first post-9/11 DBT was issued May 20, 2003, though limited "interim guidance" on upgraded security measures and several drafts of the DBT had been released before. See U.S. Congress, Government Accountability Office, *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat* (GAO, 200423 December 2006).

facilities have until late 2008 – seven years after the attacks – to comply with the new requirements.[33]

The more extreme and better-known example of these kinds of delays is in U.S.-Russian cooperation to upgrade security for weapons-usable nuclear materials: as of the end of fiscal year 2004, some 13 years after the collapse of the Soviet Union, only a little over half of the buildings with weapons-usable nuclear material in the former Soviet Union had yet had U.S.-sponsored security upgrades completed.[34] In mid-1995, when President Bill Clinton was briefed on the problem of inadequate security for nuclear stockpiles in the former Soviet Union and was told of a dispute between the Department of Defense and DOE over who would pay for particular activities that had delayed upgrades at one vulnerable site for several months, he told his national security advisor: "I want that resolved by Friday." In fact, the dispute in question was not resolved for another year.[35] The problem, of course, is that terrorists and other potential adversaries may act, react, and adapt far more quickly than the global nuclear security system does.

Both at the national level and at the international level, the nuclear security system also appears to exhibit some lock-in, or ratcheting, effects – in both directions. Once a particular rule or approach on nuclear security has been put in place and become generally accepted, it becomes quite difficult to change. It is difficult to make the rule more stringent, because the regulated parties will resist and major investments will have already been made on the basis of the rule as it stands; in most cases, some kind of major incident or external pressure is needed before decisions are taken and followed through to make nuclear security rules significantly more stringent. (Although various parties had been pressing NRC to require U.S. nuclear facilities to be defended against truck bombs for years, particularly after the 1982 destruction of the U.S. marine barracks in Lebanon by a massive truck bomb, NRC did not put such a requirement in place until 1994, after the 1993 World Trade Center bombing and the incident in which a mentally disturbed person crashed his car through the gate at Three Mile Island and disappeared into the plant for hours before he was found.) It is also difficult to make a nuclear security rule much less stringent, as this inevitably requires arguing that some security measures considered important before are no longer needed; particularly in the post-9/11 world, this is usually a very difficult case to make. Thus, there is some degree of a ratchet effect in the system, which counters to some extent the tendency to drift shown in Figure 5.2. At the same time, however, modest changes in the rules, going in

---

[33] See discussion in U.S. Congress, Government Accountability Office, *Nuclear Security: Doe's Office of the Undersecretary for Energy, Science, and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat* (Washington, D.C.: GAO, 2005; available at http://www.gao.gov/new.items/d05611.pdf as of 18 August 2005).

[34] Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 2 January 2007), pp. 27-43.

[35] Author's personal experience. This was a briefing that John P. Holdren and I gave, in May 2005, on the results of Panel on U.S.-FSU Cooperation to Protect, Control, and Account for Weapons-Usable Nuclear Materials, President's Committee of Advisors on Science and Technology, *Securing Weapons-Usable Nuclear Materials in the Former Soviet Union: Urgent Measures to Prevent Nuclear Proliferation (U).* Secret/Noforn (Washington, D.C.: Office of Science and Technology Policy, 1995).

both directions, can often get in "under the radar screen," and, when accumulated over a period of time, can mean significant drift of the system toward a different state – usually toward less protection.

An Example of System Behavior Within One Country

The classic system behavior of event leading to policy initiative leading to policy resistance can be seen in countless nuclear security controversies over the years. Consider, to take just one example, the history of efforts to actually test the performance of overall facility security systems with groups of testers pretending to be terrorists attempting to shoot their way in – so-called "force-on-force exercises" – at facilities regulated by the NRC in the United States. Realistic performance testing can play a very critical role in maintaining a strong nuclear security program, identifying vulnerabilities that need to be fixed and which were not apparent on paper; highlighting the reality of the threat and of the difficulty of defending against it, for plant management and staff (and thereby undermining complacency); providing clear evidence of the need for additional security measures to senior officials who might be less convinced by the results of computer vulnerability analyses or expert judgment; giving facilities reason to invest in additional security measures and training, in preparation for the test, in order to do well; and generally focusing regulation on real security performance, rather than on compliance with particular rules that may or may not lead to a high-performing system overall.[36]

NRC first imposed a requirement that facilities have security arrangements able to defend against a particular specified threat (known as the Design Basis Threat, or DBT) in 1979. The first reviews intended to assess whether facilities' security arrangements would in fact be able to defeat the DBT, known at the time as the Regulatory Effectiveness Reviews (RERs), began two years later, in 1981.[37] The NRC had been created by Congress a few years before, in an atmosphere of broad public concern over the safety and security of nuclear energy and the problematic nature of the Atomic Energy Commission's dual role as promoter and regulator of these technologies.[38] Moreover, the newly created DOE had established a DBT and a program of force-on-force exercises to test security at its sites in the late 1970s. The testing program rapidly found a wide range of weaknesses at DOE sites. When, in 1981, a new administration more focused on Cold War weapons production and concerned about security cost canceled the testing program, Congress, which had been conducting extensive

---

[36] For a discussion of the importance of performance testing and the difficulties with it, see Bukharin, Bunn, and Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union*; Bukharin, "Physical Protection Performance Testing."

[37] For a review of this history, see Bukharin, "Physical Protection Performance Testing."

[38] For an account of the breakup of the Atomic Energy Commission, the establishment of the NRC, and the forces that drove this process, see Duffy, *Nuclear Politics in America*. For a discussion of NRC's initial legislative mandate on nuclear security in particular, see, for example, Walker, "Regulating against Nuclear Terrorism."

investigations of nuclear security, intervened to ensure that it was restarted, presumably sending a message to NRC as well.[39]

Like the DOE effort, the RER program (which originally focused on security hardware and did not include force-on-force testing of the response forces) quickly found a wide range of severe weaknesses requiring correction, ranging from unprotected ventilation shafts going into vital areas to fences arranged in a way making it possible to jump over the intrusion detectors fairly easily. "At virtually every site, RER team members were able to avoid detection in several of the perimeter's zones."[40] Getting sites to resolve these hardware problems took the inspectors some years, and it was not until 1988 (almost a decade after such a testing program had first been instituted at DOE) that the RER teams began to observe force-on-force exercises to assess each site's response force capabilities.[41] By 1991, the worst problems with security hardware found in the previous decade had largely been fixed, but "significant weaknesses" remained in the sites' armed response to a possible attack.[42] As a result, the hardware testing was folded into regional inspections, and a new program, the Operational Safeguards Response Evaluations (OSREs) was launched, focused on force-on-force exercises designed to test the site's ability to defend against armed attack by outside intruders. The initiative to begin force-on-force exercises in particular was reportedly the result of heightened terrorism concerns in the aftermath of the 1991 Iraq war (in which Saddam Hussein had threatened to use terrorism against the United States).[43] The OSRE program focused on power reactors; a similar program, the Comparability Performance Evaluation Reviews (CPERs) tested the fuel cycle facilities handling large quantities of weapons-usable nuclear material.[44]

In each OSRE test, there would typically be four drills over several days in which a group pretending to be terrorist attackers, with the size, skills, weapons, and equipment specified in the DBT, would attempt to get through the facility's defenses and reach a particular target set (a set of equipment whose sabotage would cause substantial damage to the reactor core, a prerequisite for a major release of radiation).[45] In order to avoid people actually being shot during such an exercise, facilities were given extensive warning of when the exercise would occur, and both the attackers and the defenders used mock weapons rather than real guns; similarly, rather than using actual explosives to blast through walls or doors, times were assigned for such tasks based on earlier tests involving real explosives. Each drill typically lasted only a few minutes before either the defenders had successfully fought off the

---

[39] Bukharin, "Physical Protection Performance Testing," p. 25. See also discussion in Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Nuclear Security Coverup*, U.S. Congress, House of Representatives, 98th Congress, 2nd Session, 3 February 1984.
[40] Bukharin, "Physical Protection Performance Testing," p. 23.
[41] Bukharin, "Physical Protection Performance Testing," p. 26.
[42] Bukharin, "Physical Protection Performance Testing," p. 23.
[43] Paul Leventhal, "Testimony of Paul Leventhal on Behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force, to the Nuclear Regulatory Commission" (Washington, D.C.: Nuclear Control Institute, 5 May 1999).
[44] Bukharin, "Physical Protection Performance Testing," p. 23.
[45] Bukharin, "Physical Protection Performance Testing," pp. 23-24.

attackers, or failed to do so – because of the speed at which it is possible to climb fences, blast through walls or doors, and the like.

Like the earlier RER tests, the OSREs rapidly revealed a wide range of vulnerabilities. In over 40 of the drills conducted by May 1999, at 27 plants of the 58 reviewed by that time, the defenders failed to protect the critical target set from being destroyed by the attackers – that is, the plants were not able to fulfill their regulatory obligation to be able to defend against the DBT.[46]

As can be imagined, many in the nuclear industry did not appreciate the OSRE program. The test failures were seen as giving embarrassing ammunition to anti-nuclear critics and possibly undermining the morale and professional standing of the security managers and security forces. Industry representatives complained that the tests were expensive and disruptive to prepare for; that the practice of giving the attackers extensive information about the plant's security plan (done because the DBT included possible help from an insider, and it was assumed the attackers might get such information from an insider) was unfair; that the tests did not adequately take into account the plant staff's potential ability to mitigate the results of a sabotage after it occurred, avoiding a radioactive release; and more.[47]

The nuclear facilities subject to OSREs therefore worked to ensure that they would be conducted in a way that would have the minimum negative impact. Many aspects of the OSRE approach that the NRC ultimately adopted limited its effectiveness:[48]

- Facilities were not only warned months in advance of when the tests would take place, but were allowed to beef up their security systems and have more guards on duty for the test than they normally would – and then were not required to maintain those beefed-up capabilities after the test. Thus, the tests were often testing a security system that was significantly better than what was actually available at the plant day-to-day.
- The members of the attacking forces were not trained in the best tactics for getting through barriers, protecting themselves from defender's fire, and the like.
- The facilities, to a large extent, were able to choose the members of the attacking team, which often included members of the facility management and guard force, who had a vested interest in seeing the facility do well in the test.
- At many sites, the tests did not make use of realistic mock weapons (such as the Multiple Integrated Laser Engagement System (MILES) used for similar testing at DOE and in the military), but instead relied on rubber guns, making it very difficult for the test judges to

---

[46] Bukharin, "Physical Protection Performance Testing," p. 24.

[47] These complaints are discussed briefly inBukharin, "Physical Protection Performance Testing," pp. 24-25. See also Edwin S. Lyman, "Radiological Sabotage at Nuclear Power Plants: A Moving Target Set," in *Proceedings of the 41st Annual Meeting of the Institute for Nuclear Materials Management, New Orleans, Louisiana, 16-20 July 2000* (Northbrook, Ill.: INMM, 2000; available at http://www.nci.org/e/el-inmm2000.htm as of 18 August 2005).

[48] Except where otherwise noted, the points below are from U.S. Congress, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened.*

determine when an attacker or a defender should be considered to have been shot. (In this respect, even paintball guns would be an improvement.)

- The possibility of an insider who would actively participate with the attackers, taking actions such as disabling intrusion detectors or shooting guards from within, rather than merely providing information to the attackers, was included in the DBT the plants had to defend against, but was never tested.[49]
- The tests were quite rare, typically occurring only once every eight years at each plant – thus making it difficult to observe security trends and nip security problems in the bud.[50]
- Facilities where the defenders did not succeed in protecting the target set suffered no consequences; although the NRC's regulations required facilities to put in place security systems designed to be able to defeat the DBT, failing to do so was not considered an enforceable violation of rules if the facility fulfilled its NRC-approved security plan.[51]

Given these constraints on the realism of the OSRE tests and given the very small size of the attacking force used in these tests (while the pre-9/11 DBT is officially not public information, it is widely reported to have been three outside attackers),[52] it is remarkable that such a substantial fraction of the sites did not succeed in protecting the vital targets.

After several years, the industry became sufficiently unhappy with the OSRE tests that they began to attempt to get the program canceled. Advocates for a strong nuclear security program were fortunate that the program ended up being managed by a former military officer who was very dedicated to nuclear security, David Orrick, who defended the effort tenaciously. Nevertheless, in 1998, NRC decided to terminate the OSRE effort. Orrick filed a dissent to this decision, and the controversy within the NRC leaked to the *Los Angeles Times,* which ran a major story under the headline "U.S. Drops Anti-Terrorist Tests at Nuclear Plants."[53] This press account caused a stir in Congress, among interested non-government organizations, and at the White House, which successfully urged the NRC (which, in the U.S. system, is independent and does not have to follow White House directives) to reinstate the program.[54]

The industry and the NRC then began to develop an alternative approach that would substitute for the OSREs, in which the NRC-observed OSREs would be replaced by an industry self-assessment program. (Originally called the "Self-Assessment Program" or SAP,

---

[49] Lyman, "Radiological Sabotage at Nuclear Power Plants."
[50] U.S. Nuclear Regulatory Commission, "NRC Response to Letters to NRC Chairman Nils J. Diaz Regarding Security at Nuclear Power Plants" (Washington, D.C.: NRC, October 2004; available at http://www.nrc.gov/reading-rm/doc-collections/for-the-record/2004/nsir-response.pdf as of 18 August 2005).
[51] Leventhal, "Testimony of Paul Leventhal on Behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force, to the Nuclear Regulatory Commission".
[52] Daniel Hirsch, "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.thebulletin.org/article.php?art_ofn=jf02hirsch as of 8 January 2007), pp. 38-44.
[53] Frank Clifford, "U.S. Drops Anti-Terrorist Tests at Nuclear Plants Security: Shrinking Budget Is Cited: Simulated Attacks Had Found Serious Lapses at Half of Nation's Reactors," *Los Angeles Times*, 3 November 1998.
[54] Lyman, "Radiological Sabotage at Nuclear Power Plants."

this was eventually labeled the "Safeguards Program Assessment" or SPA.) The original plan for this effort was drafted by the industry's lobbying group, the Nuclear Energy Institute. While the revised plan did call for the tests to be conducted more frequently (every three years rather than every eight), the industry sought to include a much more demanding definition of when the attackers could be considered to have succeeded and to take credit for actions operators might take to save the plant from a major release, even though the operators' ability to perform these actions in such a crisis had never been tested, and in the event there might be armed terrorists actively preventing them from taking these actions.[55] Outside critics criticized this plan as likely to greatly undermine the realism of the OSREs, putting the testing even more firmly in the hands of people with a vested interest in ensuring that the plants would pass.[56]

Nevertheless, SPA was in the process of replacing the OSRE effort when the 9/11 attacks occurred. At that point, SPA as originally conceived was abandoned. All tests were called off for a period after the 9/11 attacks, in order to deal with other security upgrades being undertaken at the time. "Pilot" versions of a new approach began in 2003, and graded exercises resumed in 2004. Under the new approach, tests will occur every three years at each reactor, rather than every eight; the tests will use MILES equipment for enhanced realism; the new, larger DBT will be tested; and the NRC has set standards to ensure that the adversary force in the tests is trained in appropriate terrorist tactics.[57] As part of this new approach, however, the NRC went ahead and put the industry in charge of conducting the tests and did not object when the industry chose Wackenhut, the firm that provides the security forces for roughly half the U.S. nuclear power plants, as the firm to provide the attacking forces for the tests – so that Wackenhut will, in effect, be testing its own performance. Although NRC required the industry to ensure that the part of Wackenhut providing the attacking force would be independent of the part providing the guards, this provoked howls of protest from some non-government organizations and members of Congress. Those criticisms, however, do not appear to have had any effect on the outcome.[58]

This history provides a classic illustration of the policy resistance cycle in the nuclear security system. Initial concern in the 1970s, provoked in part by major terrorist attacks around the world, led NRC to put in place a DBT and later to begin increasingly extensive reviews to assess whether facilities could successfully defend against it; but by the time the force-on-force exercises got under way, it was years later and much of the initial public concern and congressional pressure had dissipated. Industry objected to the new efforts and worked with NRC first to ensure that the testing program was sharply limited and then sought to get it canceled outright. That cancellation proved a bridge too far, provoking policy

---

[55] Lyman, "Radiological Sabotage at Nuclear Power Plants."
[56] Lyman, "Radiological Sabotage at Nuclear Power Plants."
[57] See, for example, U.S. Nuclear Regulatory Commission, "NRC Response to Letters".
[58] For discussions, see, for example, Matthew L. Wald, "Battle Swirls on Security at a-Plants," *New York Times*, 6 August 2004 (available at http://pogo.org/m/hsp/hsp-nytimes-08062004.pdf as of 18 August 2005); U.S. Nuclear Regulatory Commission, "NRC Response to Letters"; Danielle Brian and Peter Stockton, "POGO Presentation to NRC Security Inspectors" (Washington, D.C.: Project on Government Oversight, 16 December 2004; available at http://pogo.org/m/hsp/hsp-NRCPhysSecInsp-041216.pdf as of 5 January 2007).

resistance on the other side, seeking to drag the system back toward its previous state. Industry then worked with the NRC to develop a new approach whose intrusiveness industry could control. That effort was interrupted by the 9/11 attacks, which provoked sufficient public and government concern that industry and the NRC moved forward with a much more extensive approach to the sort of performance testing that the industry had sought to cancel – but still took a decision to put industry in charge of the testing program and to have the same firm provide both the testers and many of the tested. In short, the concerns provoked by major incidents such as 9/11 *do* move the system toward a higher-security state – but this takes time, and policy resistance limits the magnitude of the shift.

System Constraints II: Secrecy and Sovereignty

Two additional key constraints on efforts to effect substantial improvements in the performance of the global nuclear security system are secrecy and sovereignty; with respect to international cooperation to improve nuclear security, the two are closely related.

Secrecy permeates every aspect of the global nuclear security system. There is good reason for this secrecy: no one wants to provide information that would be helpful to terrorists in organizing their efforts to steal nuclear material or build a nuclear bomb. Denis Flory, then head of the nuclear security regulatory agency in France and chairman of the international experts group that negotiated proposed amendments to the Convention on Physical Protection of Nuclear Material, put the issue in stark terms: "if in Nuclear Safety, transparency is an obligation, in Physical Protection, it is an offence."[59]

Secrecy constrains efforts to improve nuclear security, both within individual countries and internationally. Within countries, it is well-understood that government activities conducted in secrecy are often done less well than those in the sunlight; secrecy inevitably means less oversight and fewer people keeping an eye on the progress of an effort, which can allow a wide range of problems, from sloppy thinking and implementation to outright corruption, to fester uncorrected. As the Moynihan commission on government secrecy put it:[60]

> Secrecy has the potential to undermine well-informed judgment by limiting the opportunity for input, review, and criticism, thus allowing individuals and groups to avoid the type of scrutiny that might challenge long-accepted beliefs and ways of thinking. Some form of "sunlight" that permits views to be challenged while they are still in the formative stage can help reveal any institutional biases or preconceived ideas about how to approach a particular issue.

In the United States, more information related to nuclear security is made publicly available than in virtually any other country (though this openness has been scaled back

---

[59] Denis Flory, "Revising the CPPNM: Challenges and Constraints," in *Proceedings of the 44th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 13-17 July 2003* (Northbrook, Ill.: INMM, 2003).

[60] Daniel Patrick Moynihan, chair, *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2 (Washington, D.C.: Government Printing Office, 1997; available at http://www.fas.org/sgp/library/moynihan/ as of 18 August 2005).

substantially since the 9/11 attacks). There is almost certainly some information that would be useful to terrorists that has been released. But at the same time, the availability of at least limited information has made it possible for the Congress, the media, and non-government organizations to intervene repeatedly to push for action to address nuclear security vulnerabilities. The *net* effect of this somewhat greater openness has almost certainly been greater security than would otherwise have been the case.[61]

Internationally, secrecy is a very fundamental constraint on any effort to cooperate to improve nuclear security. Secrecy concerning how large nuclear stockpiles are and at what sites and buildings they are located makes it extraordinarily difficult to assess the size of the problem and plan programs to address it. Secrecy concerning the specific security arrangements in place makes it extremely difficult to assess whether those arrangements need to be strengthened. Secrecy that makes it difficult or impossible for foreigners to visit relevant sites enormously complicates efforts to assist or cooperate in upgrading security at those sites – and in particular to confirm that the donor state's taxpayer's funds are being spent appropriately – a problem that has continually plagued U.S.-Russian cooperation to improve security and accounting for nuclear stockpiles[62]. Secrecy limits the opportunities for transparency measures that would help identify security weak points requiring corrective action; that might encourage states to fix embarrassing problems before opening themselves to review; and that could identify when thefts have occurred, or confirm that all material was present and accounted for.[63] For example, although international peer reviews of safety at nuclear facilities are common, international peer reviews of security and a suggestion to include a provision making them mandatory in an amended physical protection convention was rejected by nearly all the parties participating in the discussions.

Similarly, states' efforts to protect their sovereignty over nuclear security matters have tightly constrained efforts to set binding international rules for nuclear security. Among the major powers particularly, each has its own approach to nuclear security and none is interested in being told what to do by the others. This emphasis on each state maintaining complete freedom to control its own nuclear security affairs has made it extremely difficult to reach agreement on any form of binding international standards for nuclear security, or any form of mandatory international peer review that might imply judgments that nuclear security in a particular country was not being handled as well as it should be. In particular, by a stroke

---

[61] Of course, just as nuclear industry officials have strong incentives to convince themselves that expensive additional security measures are not needed, I have a strong incentive to convince myself that some degree of transparency with respect to nuclear security is desirable, since a dissertation like this one (along with much of my other work) would not be possible without it. The reader should keep this likely bias in mind.

[62] For discussions, see Bukharin, Bunn, and Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union*; Matthew Bunn, "Cooperation to Secure Nuclear Stockpiles: A Case of Constrained Innovation," *Innovations* 1, no. 1 (2006; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/INNOV0101_CooperationtoSecureNuclearStockpiles.pdf as of 4 April 2006).

[63] For a discussion of these points, see, for example, U.S. National Academy of Sciences, Committee on International Security and Arms Control, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials* (Washington, D.C.: National Academy Press, 2005; available at http://books.nap.edu/catalog/11265.html as of 8 August 2005).

of historical bad luck, the second half of the 1970s, the time when the United States first began attempting to convince other states to agree on stringent nuclear security standards, was also the time when the United States reversed its position on the back end of the nuclear fuel cycle, abandoning reprocessing and attempting to convince others to do likewise. Since then, other countries that continued to pursue reprocessing (including the major European powers, Japan, and Russia) have often regarded U.S. attempts to ensure that high standards of security were maintained for weapons-usable materials such as separated plutonium as a back-door means of interfering with their fuel cycle choices. This attitude has contributed to their insistence that nuclear security is a matter of national sovereignty and should not be controlled in detail by international agreements and organizations.[64]

An International Example of System Behavior: Responding to 9/11

The reaction to the 9/11 attacks provides a useful current example of the behavior of the nuclear security system at the international level. The attacks immediately aroused public and government concern over whether security for nuclear security was sufficient, in countries around the world.

At first it appeared that this event – a carefully planned suicide attack involving 19 individuals in four independent but well-coordinated teams, succeeding in killing over 3,000 people and striking both the World Trade Center and the Pentagon, global symbols of American economic and military power – would be enough to shock the global nuclear security system into taking action to protect nuclear facilities against threats of comparable magnitude (for example, 19 well-trained, well-equipped attackers in several teams). In the United States, DOE immediately beefed up guard forces at nuclear facilities, and several governors sent National Guard units to guard nuclear facilities (though others did not).[65] In France, air defense missiles were deployed to protect the La Hague reprocessing facilities from attacks by hijacked aircraft.[66] In Japan, units of the national police were deployed to provide the first armed guards for nuclear facilities.[67] In Russia, Britain, and elsewhere, additional armed guards were deployed to protect nuclear facilities, controlled areas around facilities were widened, and other steps were taken to heighten security. Russian officials publicly warned that terrorist teams had been carrying out reconnaissance at Russian nuclear warhead storage facilities,[68] and Alexander Rumiantsev, then Minister of Atomic Energy, agreed with U.S. Secretary of Energy Spencer Abraham that the two sides should accelerate their efforts to install improved security and accounting systems at Russian nuclear sites.[69] At

---

[64] For a good discussion of these issues, see Scheinman, "Transcending Sovereignty."
[65] Matthew Bunn, "Nuclear Security in the United States: Response to 9/11" (unpublished: 3 February 2005).
[66] "French Air Force Installs Radar System at Nuclear Site," *Agence France-Presse*, 19 October 2001.
[67] Tatsujiro Suzuki, "Implications of 09/11 Terrorism for Civilian Nuclear Industry and Its Response Strategy," paper presented at Japan Atomic Industrial Forum-Harvard University Nonproliferation Workshop, Cambridge, Mass., 30-31 January 2002.
[68] "Russia: Terror Groups Scoped Nuke Site," *Associated Press*, 25 October 2001; Pavel Koryashkin, "Russian Nuclear Ammunition Depots Well Protected – Official," *ITAR-TASS*, 25 October 2001.
[69] U.S. Department of Energy, "U.S. And Russia Agree to Strengthen Nuclear Material Protection" (Washington, D.C.: DOE, 29 November 2001; available at http://www.energy.gov/HQPress/releases01/novpr/pr01200_v.htm as of 9 January 2003).

a summit meeting two months after the attacks, U.S. President George W. Bush and Russian President Vladimir Putin called for "urgent attention" to improving physical protection of nuclear weapons and nuclear materials.[70]

Despite the IAEA's usual practice of caution and of waiting until all the views of the member states could be heard and weighed, IAEA Director-General Mohammed ElBaradei issued a sweeping statement warning that "September 11 presented us with a clear and present danger and a global threat that requires global action." Pointing out that "nuclear security is only as strong as its weakest link," and that "radiation knows no frontiers," ElBaradei called for major modifications of the traditional approach of putting nuclear security exclusively in the sovereign hands of each state, saying that an "unconventional response" was needed, in which "the whole world needs to join together and take responsibility for the security of nuclear material." Strongly implying that some form of international system to verify that adequate nuclear security measures were in place was needed, ElBaradei argued that "countries must demonstrate, not only to their own populations, but to their neighbors and the world that strong security systems are in place.... Countries will have something to gain from allowing international assessments to demonstrate to the world that they are keeping their nuclear material secure." ElBaradei indicated that an IAEA program costing "at least $30-$50 million annually" was needed to meet the new threat.[71]

But the system constraints of complacency, policy resistance, sovereignty, and secrecy remained very much in place. Most of the key officials in most states considered public concerns over the nuclear terrorism threat to be overblown and the need for additional security measures to be modest. Few states had any interest in compromising on the traditional emphasis on secrecy and exclusive national sovereignty in managing security for nuclear stockpiles, even if allowing some international intrusions on their sovereignty and secrecy might lead to increased confidence that that other countries were putting appropriate nuclear security measures in place.

The commercial nuclear industry was placed in a difficult position by the wave of public concern over nuclear security following the attacks. The industry took three tacks: emphasizing the high levels of security already in place and the low likelihood that an attack on a nuclear facility would be successful (including, in the heat of the moment, a number of statements from industry spokesmen that were patently false – such as the claim by a representative of the Nuclear Energy Institute that U.S. nuclear facilities were "more secure than Fort Knox," the major U.S. gold depository);[72] offering public support for improved

---

[70] "Joint Statement on New U.S.-Russian Relationship" (Crawford, Texas: The White House, Office of the Press Secretary, 13 November 2001; available at http://www.whitehouse.gov/news/releases/2001/11/20011113-4.html as of 22 August 2005).

[71] International Atomic Energy Agency, "Calculating the New Global Nuclear Terrorism Threat" (Vienna: IAEA, 1 November 2001; available at http://www.iaea.org/NewsCenter/PressReleases/2001/nt_pressrelease.shtml as of 16 September 2005).

[72] Michael Mansur, "Nuclear Plant Security Stirs Concern," *Kansas City Star*, 18 September 2001. To be fair, anti-nuclear critics offered a number of assessments of nuclear security in the weeks following the 9/11 attacks that were equally wide of the mark.

security measures;[73] and working behind the scenes to ensure that the new measures did not go too far, from the industry's perspective.

Because of these types of policy resistance from many of the key states in the global nuclear security system and from their nuclear industries, the actual international response to the 9/11 attacks has fallen far short of ElBaradei's vision. As discussed in more detail below, suggestions to set specific standards for nuclear security internationally (based on the IAEA's recommendations in this area); to call for international peer reviews of nuclear security in individual countries; and even to establish a system of reporting about nuclear security (in which states would have been able to report at whatever level of detail they felt comfortable with) were all summarily rejected by experts negotiating a draft amendment to the convention on physical protection of nuclear material as representing too great an intrusion on secrecy and sovereignty, just as they had been before the 9/11 attacks.[74] Even so, the amendment to the physical protection convention was not approved until mid-2005, almost four years after the 9/11 attacks, and it will be several years more before it enters into force.[75] Similarly, after delaying for years both before and after the 9/11 attacks, the United Nations finally approved a convention on nuclear terrorism in mid-2005, nearly seven years after it had first been proposed – but it includes no provisions requiring states to provide high security for their nuclear material, the most effective means to prevent nuclear terrorism.

In April 2004, the UN Security Council did pass Resolution 1540, legally requiring every UN member state to provide "appropriate effective" security for their nuclear stockpiles (among other things) and to report on what it has done to implement the resolution. While this is potentially very promising, as of late 2006 there had been no effort to define what the essential elements of an "appropriate effective" nuclear security system were and to convince states to put them in place. Neither the United States nor any other major exporter (or the Nuclear Suppliers Group) has tightened its requirements for physical protection of the nuclear material it exports. In short, states today face few more international requirements for or constraints on their approach to nuclear security than they did before the 9/11 attacks occurred.

Nor has the IAEA's response gone as far as the agency once hoped. The IAEA Board of Governors approved the general outlines of the agency's proposed program to counter nuclear terrorism, but refused to include such measures in the agency's regular budget, forcing the agency to rely on voluntary contributions to fund this work. As of mid-2005, the Nuclear Security Fund had spent $19.5 million in the nearly four years following the 9/11 attacks – far more than had been available for such purposes previously, but substantially less

---

[73] See, as one of many examples, World Nuclear Association, "World Industry Lauds IAEA Initiative on Nuclear Safety and Security" (London: WNA, 2 November 2001).
[74] Flory, "Revising the CPPNM: Challenges and Constraints."
[75] Patricia A. Comella, "Revising the Convention on the Physical Protection of Nuclear Material--Chapter VI," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

than the amount the IAEA had argued after 9/11 was necessary for a single year.[76] (For context, extensive security and accounting upgrades at a single building typically cost in the range of $10 million.) Within the agency, a great deal of time has been spent on squabbling over where the boundary between safety and security lies; on how many resources to devote to protection against nuclear theft, nuclear sabotage, and misuse of radiological sources; and over who would have control over the nuclear security efforts.[77]

Individual states, in many cases, *have* made substantial improvements in nuclear security in the months and years since 9/11 – because they chose to do so for their own reasons. But in other states, little has changed, and there has been precious little of the whole world joining together for global action, as ElBaradei envisioned. ElBaradei's call for states to demonstrate to each other and the world that their nuclear security systems are effective has been almost entirely ignored. In short, rather than the bold and "unconventional" response ElBaradei envisioned, the international response to 9/11 has been quite conventional – highlighting the difficulty of overcoming the system's constraints, even in response to a major incident.

Policy Tools for Improving System Performance

Reduced risk of nuclear theft and terrorism is the obvious measure of performance improvements in the global nuclear security system. The cost of those improvements is also important (particularly as perceptions of that cost will lead to policy resistance that will create important constraints on the ability to reduce risk). But if the parameter values used as examples in the nuclear terrorism risk model in Chapter 3 are remotely close to representing reality, the costs of proposed nuclear security measures are modest by comparison to the reductions in expected losses that might be achieved. The costs of nuclear security are certainly quite modest if compared to the sums states routinely pay to improve their military security, or to the revenue generated from nuclear energy.

Faced with a system with hundreds of almost entirely independent nodes, failure of any one of which could lead to catastrophic system failure, an engineer asked to suggest steps to reduce the risk of system failure would recommend: (a) reducing the failure risks of individual nodes (especially the highest-risk ones); (b) reducing the number of nodes (preferentially eliminating the highest-risk ones); and (c) increasing the system's capacity to identify high-risk nodes and to cause them to reduce the risks they pose. With respect to the global nuclear security system, these approaches correspond to recent recommendations to urgently upgrade security measures for nuclear stockpiles worldwide; to undertake a rapid "global cleanout," removing weapons-usable nuclear material entirely from as many sites as

---

[76] International Atomic Energy Agency, "States Agree on Stronger Physical Protection Regime" (Vienna: IAEA, 8 July 2005; available at http://www.iaea.org/NewsCenter/PressReleases/2005/prn200503.html as of 22 August 2005).

[77] Interviews with IAEA officials, November 2001, September 2002, May 2003, June 2004, and May, September, and October 2005. For a recent assessment of the IAEA nuclear security program, see U.S. Congress, Government Accountability Office, *Nuclear Nonproliferation: IAEA Has Strengthened Its Safeguards and Nuclear Security Programs, but Weaknesses Need to Be Addressed*, GAO-06-93 (Washington, D.C.: GAO, 2005; available at http://www.gao.gov/new.items/d0693.pdf as of 10 May 2006).

possible worldwide; and to create stringent global standards of nuclear security, with some mechanism for international organizations or states in the international community to confirm that states are complying.[78]

The system behavior just described, however, suggests that the obstacles to implementing such proposals are substantial. The United States and other participants in the global nuclear security system have tried a variety of policy tools to improve system performance over the years, including: seeking to negotiate binding global nuclear security standards; working out non-binding international recommendations and encouraging states to follow them; organizing voluntary international peer reviews; providing various types of international training and advice; imposing requirements for nuclear security as a condition of nuclear supply; improving nuclear security and accounting measures at individual sites through direct technical cooperation; and seeking to remove nuclear weapons or weapons-usable material entirely from particular high-risk sites. What does the record say about how effective these different policy tools are, under what circumstances? A full exploration of this history, providing convincing tests of different hypotheses as to what caused the outcomes observed, is beyond the scope of this chapter (and likely beyond the scope of the available data as well). The discussion below, therefore, is no more than a best judgment as to the factors that limited the success of some policy tools and contributed to the progress made by others.

Criteria are needed to compare the relative efficacy of the different policy tools as they have been attempted so far. The discussion below will employ three principal criteria: the *speed* of any improvements in nuclear security resulting from the use of a particular policy tool; the *security level* achieved through the use of that policy tool; and the *breadth of applicability* of that tool. Each of these is a crucial ingredient of effectiveness: speed is key, as even substantial nuclear security improvements, if they took decades to implement, might not come in time; security level is equally crucial, for even rapid and broadly implemented security improvements might not solve the problem if the improvements were minimal and did little to reduce the probability that terrorists and thieves could overcome them; and breadth of applicability is another essential ingredient, as even substantial security upgrades, implemented rapidly, might do little to address the threat if they could be implemented at only a small fraction of the sites requiring upgrades. There may be trade-offs among these criteria, however: measures that are more broadly applicable, for example, may be less effective in leading to large and rapid improvements at particular sites.

Each policy tool will be given a 1-5 rating on each of these criteria, as follows:

Speed:

1: 20 years or more between the time when an attempt to use a policy tool was initiated and when significant improvements in actual nuclear security arrangements occurred

2: 10 years or more between initiation and significant improvements

---

[78] For recent recommendations in all three of these areas, see Bunn and Wier, *Securing the Bomb 2005*; Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004).

3: 5-10 years between initiation and significant improvements, or possibility that such a pace could be achieved with that tool with a different approach
4: 2-5 years between initiation and significant improvements, or possibility that such a pace (or an even faster pace) could be achieved with that tool with a different approach
5: Less than 2 years between initiation and significant improvements

Security Level:
1: Minor improvement in risk of nuclear theft
2: Noticeable improvement, but sites likely still vulnerable to even a small group of determined attackers, or 1-2 well-placed insiders
3: Substantial improvement, but sites likely still vulnerable to well-planned attacks by a modest group of attackers, or 1-2 well-placed insiders, or both working together
4: Major improvement, sites probably protected against attacks by modest groups of outside attackers, 1-2 well-placed insiders, or both working together
5: Dramatic improvement, sites probably protected against squad-size force of well-trained and well-armed attackers, 1-4 well-placed insiders, or both working together. (This corresponds roughly to the new rules DOE facilities are being required to meet over the next few years; few nuclear facilities in other countries are believed to be intended to be protected at this level.)

Breadth of Applicability:
1: Successfully applied only to 0-9 facilities, little likelihood of broader application.
2: Successfully applied or likely to be applicable to only a small fraction of the facilities with nuclear weapons or weapons-usable nuclear material worldwide.
3: Successfully applied or likely to be applicable to a substantial fraction of the facilities with nuclear weapons or weapons-usable nuclear material worldwide, but major classes of facilities (e.g., all military facilities, or all facilities in countries outside the NPT) excluded.
4: Successfully applied or likely to be applicable to the majority of facilities with nuclear weapons or weapons-usable nuclear material worldwide.
5: Successfully applied or likely to be applicable to all or nearly all facilities with nuclear weapons or weapons-usable nuclear material worldwide.

Binding Multilateral Agreements

As described earlier in this chapter, a series of events and trends in the early-to-mid-1970s, particularly the 1972 attack on the Munich Olympics and public concern about the growth of nuclear energy, contributed to a sharp increase in concerns about the possibility of nuclear terrorism, particularly in the United States. It was in this context that in 1974, the Ford administration proposed negotiating an international convention on security for nuclear material; at the time, Secretary of State Henry Kissinger emphasized that such a "convention should set forth specific standards and techniques for protecting materials," whether in

domestic use or in international transport.[79] The final declaration of the 1975 review conference for the Nonproliferation Treaty called on all states engaged in peaceful nuclear activities to "enter into such international agreements and arrangements as may be necessary" to ensure effective physical protection for nuclear material worldwide.[80]

After some preliminary meetings, the United States proposed a draft text of an agreement in mid-1977.[81] The U.S. draft would have covered all civilian nuclear material and facilities; would have required not only measures to prevent theft, but steps to prevent sabotage as well; and would have required all parties to provide "appropriate measures" to prevent theft and sabotage, citing the IAEA's physical protection recommendations as a "useful basis for guiding" states in putting appropriate physical protection in place. Even this initial U.S. draft was far weaker than previous statements had suggested. It included none of Kissinger's "specific standards and techniques," specifying no particular security measures to be taken or specific threat to be defeated; it excluded all military nuclear materials (which were even more dominant in the world's nuclear stockpiles then than they are today); and it did not include any verification or compliance measures.[82] It appears that this initial draft represented a U.S. estimate of the most that might potentially be negotiable.

As it turned out, this estimate was incorrect. While some countries argued for going further than the U.S. draft (for example, extending it to cover military materials and specifying minimum security measures to be taken), others argued that it intruded too far into national sovereignty over control of nuclear materials and that it was unwise to even refer to the IAEA recommendations as a guide, as this would effectively make them mandatory (or so it was argued). In the end, a decision was taken to pursue a convention with a scope that could get support from the largest number of countries participating in the talks. Hence, the final convention, opened for signature in 1980, only required physical protection measures for nuclear material in international transport (the area that all agreed was a legitimate concern of the international community), excluding material in domestic use from the physical protection requirements and did not refer at all to the IAEA recommendations. (The bulk of the convention's text focuses on useful provisions requiring states to cooperate in the event of a real theft and establishing procedures for arresting and trying those who participate in real or attempted nuclear thefts, whichever party to the agreement may catch them.)

What specifics there are on security for material in international transport in the final convention are extremely broad: states are required to take "appropriate steps" to ensure "as

---

[79] Kissinger's remarks, in a speech to the UN General Assembly, are excerpted in U.S. Senate, Committee on Government Operations, *Peaceful Nuclear Exports and Weapons Proliferation: A Compendium* (Washington, D.C.: Government Printing Office, 1975), pp. 553-554.

[80] The full text of the 1975 final declaration can be found in Emily Bailey et al., eds., *Briefing Book: Volume II: Treaties, Agreements, and Other Relevant Documents* (Southampton, U.K.: Programme for Promoting Nuclear Non-Proliferation, 2000).

[81] The IAEA has compiled much of the negotiating history of the physical protection convention in International Atomic Energy Agency, *Convention on the Physical Protection of Nuclear Material*, Legal Series No. 12 (Vienna: IAEA, 1982).

[82] The U.S. draft is reproduced in International Atomic Energy Agency, *Convention on the Physical Protection of Nuclear Material*, pp. 7-15.

far as practicable" that nuclear materials being transported are protected at the levels specified in an annex. The annex indicates that "Category I" material (the most sensitive weapons-usable nuclear material), when in storage incidental to international transport, should be in an area with a fence around it, which only people "whose trustworthiness has been determined" can enter, and which is under continuous watch by guards (who need not be armed) who are "in close communication with appropriate response forces." Under the convention, international transport should only take place once the shipper, receiver, and carrier have agreed on arrangements, and, for Category I materials, under "constant surveillance" by escorts in "close communication with appropriate response forces." But there is no requirement for armed guards, for systems able to defeat any particular level of threat, for any particular speed at which response forces would arrive, or for any type of intrusion detectors or portal monitors to detect removal of nuclear material. There are no specifics on how strong the fence must be or how effective the approaches to determining trustworthiness must be (and no requirement that the transport be conducted by people whose trustworthiness had been determined). These requirements are far more general and vague than the IAEA recommendations on physical protection (which were themselves quite general at the time). The convention did not gain enough parties to enter into force until 1987, and many key states (such as India, Pakistan, and Israel, among others) did not become parties until more than a decade later.[83]

In 1998, the United States took another run at the idea of creating genuine binding global nuclear security standards, proposing that the Convention be amended to (a) extend its coverage to civilian nuclear material in domestic storage, use, and transport; (b) require that at a minimum, states provide levels of protection comparable to those called for in the IAEA recommendations; and (c) require that states provide reports on their physical protection arrangements every five years, to be discussed at international conferences that would also take place every five years.[84] IAEA staff outlined additional possibilities, including provisions for protecting against sabotage of facilities as well as theft of materials and extending the convention's coverage to protection of military as well as civilian nuclear material.

The IAEA Director General then convened an experts' meeting, which, after some initial disagreement, recommended drafting an amendment to the Convention extending its coverage to civilian nuclear material in domestic use, storage, and transport; adding a requirement to protect against sabotage of nuclear facilities as well as theft of nuclear

---

[83] For the current list of parties to the convention and the dates at which they acceded, see International Atomic Energy Agency, "Convention on the Physical Protection of Nuclear Material" (Vienna: IAEA, December 2006; available at http://www.iaea.org/Publications/Documents/Conventions/cppnm_status.pdf as of 5 January 2007).

[84] For a discussion of the early stages of these discussions, see George Bunn, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," *Nonproliferation Review* 7, no. 2 (Summer 2000; available at http://cns.miis.edu/pubs/npr/vol07/72/72bunn.pdf as of 2 January 2007). For reviews of more recent discussions, see Comella, "Revising the Convention on the Physical Protection of Nuclear Material--Chapter VI.". See also the papers with the same title presented by Comella in each of the previous five years. Secretary of State Madeleine Albright first proposed amending the convention in a 1998 speech surveying the future of arms control. See Madeleine Albright, "Arms Control in the 21st Century" (Washington, D.C.: U.S. Department of State, 10 June 1998; available at http://www.clw.org/archive/coalition/albr0610.htm as of 9 May 2006).

material; stating 12 fundamental principles for physical protection that parties should follow; and including some additional issues related to confidentiality and national responsibility. As noted earlier, however, the group opposed including any requirement that states prepare any form of reports on their physical protection arrangements and regulations; any mechanism for international peer review of such arrangements; any reference to the much more detailed IAEA physical protection recommendations, even a requirement to give them "due consideration" or take them "into account"; and any extension of the convention to material in military use.[85]

Ironically, the experts group finished its work and reached these conclusions just before the 9/11 attacks took place. Those attacks led much of the world public to assume that increased security measures for nuclear facilities would be put in place, and in many countries they were. But the conclusions of the pre-September 11 experts' group that there was no need for specific binding standards, no need for any form of reporting on or review of measures in place, and no need to cover military stockpiles, were still accepted as gospel. A separate group was put together to negotiate an amendment to the convention based on the experts' group recommendations – a process that proved so contentious that the participants were unable to reach consensus on final language. Austria therefore took it upon itself to circulate a text where it put in, at each bracketed point, the language it believed had the most international support. With one modest modification, that text became the agreed amendment to the convention, which was approved at an international conference in mid-2005, seven years after the United States had first proposed such an amendment and nearly 4 years after the 9/11 attacks.

The amendment includes some useful provisions (particularly in extending the convention's criminal provisions to cover nuclear sabotage as well as nuclear theft), but it is a far cry from what advocates once envisioned or the United States once proposed. While it extends the convention's coverage to domestic material, even the extremely vague provisions on physical protection for material in international transport in the original convention were

---

[85] See discussion in International Atomic Energy Agency, *Measures to Improve the Security of Nuclear Materials and Other Radioactive Materials*, GC(45)/INF/14 (Vienna: IAEA, 2001; available at http://www.iaea.org/About/Policy/GC/GC45/Documents/gc45inf-14.pdf as of 9 May 2006). As it turned out, the United States concluded that not only were all the other participants opposed to making security measures consistent with the IAEA recommendations mandatory, the U.S. Department of Energy was as well, because DOE rules categorizing nuclear material were quite different from those recommended by the IAEA, and some material that should have had substantial protection under the IAEA recommendations was considered under DOE's rules to be in a lower category requiring minimal protection. See Marshall D. Kohen and Joseph D. Rivers, "DOE's Involvement in Negotiations on the Question of Whether to Revise the Convention on the Physical Protection of Nuclear Material," in *Proceedings of the 42nd Annual Meeting of the Institute for Nuclear Materials Management, Indian Wells, Cal., 14-18 July 2001* (Northbrook, Ill.: INMM, 2001). Indeed, by the end of the talks, the United States was, by some reports, actively opposing proposals to make the proposed amendment stronger and more specific. As one negotiator for a European country put it, "the U.S. delegation supports any proposal, as long as it is utterly ineffective." Interview, September 2002. U.S. negotiators deny, however, that DOE's opposition was influential in the U.S. decision to abandon the notion of incorporating a requirement to take the IAEA recommendations into account into the amendment, arguing that this requirement was so broadly opposed it was essential for the United States to drop the idea in order to move forward with the amendment. Interview with State Department official, July 2003.

considered too specific to be applied domestically; the amendment only requires that protection for domestic material be "appropriate" and that parties "insofar as is reasonable and practicable" follow a variety of "fundamental principles" of physical protection. These principles are extremely general, in effect requiring that states take responsibility for physical protection and establish rules for what levels of physical protection there should be, but not detailing *any* specific measures that should be taken.[86] Kissinger's "specific standards and techniques" are still nowhere to be found. The amendment will not enter into force until two-thirds of the parties have ratified it, a process expected to take years.

Similarly, as noted above, while UN Security Council Resolution 1540 legally requires all states to provide "appropriate effective" security for any nuclear stockpiles they may have, there has as yet been no national or international effort to define what that means and to ensure that states are putting the essential elements of an appropriate effective system into place.[87] And the new nuclear terrorism convention focuses primarily on criminalizing and prosecuting nuclear terrorism offenses, rather than on physical protection. Article 8 of the convention, however, does require all parties to make "every effort to adopt appropriate measures to ensure the protection" of nuclear and radioactive material, "taking into account" the IAEA's recommendations on physical protection. This reference to the IAEA recommendations, at least as something to be taken into account (if not necessarily complied with in full) is particularly interesting, as it proved impossible to get identical language in the physical protection convention amendment. In part, the explanation may be that the negotiation of the nuclear terrorism convention was largely carried out by lawyers in New York, less directly familiar with any concerns their countries' nuclear establishments may have had about the IAEA recommendations. Moreover, as the nuclear terrorism pact was a new negotiation, not an amendment to a previous one, there was no prior history of rejecting attempts to include references to the IAEA recommendations, as there was in the case of the physical protection convention.

Ratings: This effort to negotiate multilateral agreements to improve nuclear security rates badly on each of the three criteria described above.

Speed: 2

The pace was glacially slow, from a first proposal in 1974 to entry into force in 1987 for the original convention and first proposal in 1998 to entry into force still years away for the amendment. Any improvements in nuclear security rules in response to the amendment to the convention will presumably take years to work their way through the governmental processes in each country. Even the goad of the 9/11 attacks seems to have done little to accelerate the process or strengthen the amendment that was ultimately agreed.

---

[86] For the full text of the agreed amendment, see International Atomic Energy Agency, *Nuclear Security - Measures to Protect against Nuclear Terrorism: Amendment to the Convention on the Physical Protection of Nuclear Material*, GOV/INF/2005/10-GC(49)/INF/6 (Vienna: IAEA, 2005; available at http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf as of 9 May 2006).

[87] For discussion, see Bunn and Wier, *Securing the Bomb 2005*, pp. 110-112.

Security Level: 1

The level of security reached was low, since the original convention offered only very general requirements for only a tiny fraction of the world's material (that which was under international transport at any given time), and the amendment has even less specific requirements for domestic material.

Breadth of Applicability: 2-3

The breadth of application the physical protection convention negotiations have achieved was limited. The original convention applied to only a tiny fraction of the world's nuclear material – the material in international transport at any given time. Even the amendment excludes the military material that makes up some four-fifths of the world's stockpiles of weapons-usable nuclear materials. While the original convention now includes a large fraction of the states with weapons-usable nuclear material on their soil, it will be years before the same can be said of the amendment. The UNSC 1540 requirement is applicable to all the world's nuclear stockpiles, but so far has not been used to attempt to achieve significant improvements in security for these stockpiles.

Summed effectiveness rating: 5-6 (of possible 15)

While the effectiveness of this approach has been limited to date, that does not mean these efforts have had no value. In several countries, for example, advocates for putting basic physical protection regulations in place have indicated that the amended convention requiring such measures would help them convince others in their governments of the need to move forward.[88] Several tentative lessons can be drawn from this experience.

Lack of belief in the threat will stymie progress. Many states simply do not believe the threats of nuclear theft and sabotage are as urgent as the United States believed they were in the mid-1970s or after the 9/11 attacks. Seeing only modest threats to be addressed, states were not willing to agree to far-reaching steps to address them.

Differing national approaches and concerns over sovereignty make it difficult to agree on specific measures. States' desire to maintain the freedom to take whatever approach to nuclear security they think best stands out as a recurring theme of the physical protection convention negotiations. The United States believes its approaches to nuclear security are better than those of other countries; Russia believes its different approaches are equally good; France prefers its approaches; and so on. A successful global nuclear security standard would have to be specific enough to be effective, but general enough to allow each country freedom to pursue its own approach to implementation.

Lack of top-level political attention makes it difficult to push for more effective measures. Negotiations carried forward at a low political level among "experts" have tended to mean that the negotiators are closely linked to the nuclear establishments of their respective countries and do not feel they have the authority to agree to anything that would cost those establishments more money or force them to change the way they do business. Only at much

[88] Flory, "Revising the CPPNM: Challenges and Constraints."

higher political levels, or with backing from high political levels, would negotiators have the political leeway to take broader interests more effectively into account.

The search for broad support leads to weak agreements. As the talks have been structured so far, they have been built around searching for consensus, or, in some cases, for the language that provoked the fewest objections from participating states. That has inevitably driven them toward weakened, least-common-denominator approaches. This is not an inevitable aspect of multilateral negotiations. In cases where many participants believe the treaty is addressing a serious threat and where top political leaders take a personal interest in ensuring that the treaty includes effective language, stronger language is often reached in multilateral fora (the Chemical Weapons Convention and the Comprehensive Test Ban Treaty being two recent examples). In some multilateral talks, such as the negotiation of the Nonproliferation Treaty (NPT), key provisions have been worked out between the most powerful and most interested states, making it possible to develop stronger approaches. In the case of the physical protection negotiations, negotiators – virtually none of whom had themselves ever designed or operated a physical protection system – came to focus more on finding language that would bridge the gaps between different countries' proposals than on finding language that would make a real difference on the ground, if accepted.

International Recommendations

Another approach that has been pursued for decades is working through the IAEA to promulgate international "recommendations" on physical protection. The IAEA called together the first advisory group on physical protection at U.S. instigation in 1971. Led by the U.S. and Soviet representatives, but with active involvement from several other countries as well, the group quickly agreed on the first IAEA recommendations for all states on physical protection, which were published in 1972 and were known as the "Grey Book."[89]

These recommendations were revised and issued as Information Circular 225 (INFCIRC/225) in 1975. A minor first revision was published in 1977; a more substantial second revision in 1989; a minor third revision in 1993 (intended only to make slight modifications to the table for categorizing nuclear materials, so that it was consistent with the table in the physical protection convention); and the most recent revision, a substantial one that included extending the recommendations' scope to cover protection against sabotage as well as theft, was published as INFIRC/225/Rev. 4 in 1999. This most recent revision was the result of two meetings of a group of international experts, for several days each in June and October of 1998.[90] A new review, intended to produce a fifth revision of INFCIRC/225, is now beginning.[91]

---

[89] The text of the Grey Book is reproduced in U.S. Senate, *Peaceful Nuclear Exports*.

[90] See discussion in the preface of the revised recommendations, in International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected) (Vienna: IAEA, 1999; available at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html as of 22 December 2006).

[91] Interview with Anita Nilsson, head of the IAEA Office of Nuclear Security, October 2005.

The 1972 recommendations were very general (as U.S. physical protection regulations were themselves at the time), though still more specific than the physical protection convention. The recommendations have become more specific and detailed over time. INFCIRC/225/Rev. 4 contains 21 paragraphs of steps to be taken to protect Category I nuclear material. Such material should be stored and used in inner area within a building, inside a protected area with a fence or other physical barrier around it; only personnel whose trustworthiness has been determined are to be allowed access to it; whenever anyone is with such material they are to be kept under surveillance at all times; the facility should have a 24-hour guard force (and if the guards are not armed, "compensating measures should be applied"); all such nuclear material should be stored in a locked and alarmed "strong room" when not in use; there should be intrusion detectors at the perimeter of the protected area that communicate to a central alarm station manned by the guard force; the central alarm station should have "dedicated, diverse, and redundant" two-way voice communication with both the guard force and off-site response forces; the guard force should have reliable communications to appropriate armed response forces; regular tests or evaluations of the system's overall performance should be carried out; and so on. Perhaps most important, states should require facilities to put in place security arrangements and plans able to defeat a design basis threat which the state should specify.[92]

While considerably more specific than the physical protection convention, these recommendations are still extremely general – in part because countries have widely varying approaches to nuclear security, and experts from those countries, familiar and comfortable with those pre-existing approaches, did not want to agree to measures that would require them to be substantially changed. Armed guards are not necessarily required. No minimum threat to be defended against is mentioned. There is no discussion of how good the fence should be, how strong the strong-room should be, how reliable the intrusion detectors should be, how numerous the guards should be, and the like. It is certainly possible to comply with the IAEA recommendations and have a very modest level of security, not likely to be able to defeat either a determined outside attack by even a relatively small group of well-trained and well-armed adversaries, or an insider threat of, say, two well-placed and dedicated insiders working together.

This international recommendations approach rates significantly better, using the criteria described above, than the attempts to negotiate binding global standards for nuclear security.

Speed: 3

Negotiation of each version of the IAEA recommendations has generally been quick (typically one to two years or less). But implementation in individual countries has often been slow (often taking years, even for those countries that base their policies on the IAEA recommendations, to revise their approaches to reflect a new revision of the recommendations.)

---

[92] International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities.*

Security Level: 3

Those countries that follow the recommendations reach a security level significantly higher than would be ensured from following the convention alone (even if a state were to apply the convention's most specific provisions, intended only for material in international transport, for domestic material as well). But because the recommendations remain quite general, the security level ensured by complying with them remains fairly modest by comparison to the threats terrorists and criminals have shown they can pose in many countries.

Breadth of Applicability: 4

With respect to breadth of applicability, the recommendations have been surprisingly successful. Most of the countries with weapons-usable nuclear material say, in principle at least, that they comply with the IAEA recommendations. In many countries, physical protection laws and regulations are explicitly based on – in some cases essentially lifted from – the IAEA recommendations. Indeed, as discussed below, a variety of nuclear supply agreements and other bilateral undertakings effectively require a substantial number of countries to comply with the IAEA recommendations.[93] Unlike the convention, the recommendations are not specifically limited to civilian nuclear material; some countries with military nuclear material may have implemented additional security measures for those stockpiles with the IAEA recommendations in mind.

Summed Effectiveness Rating: 10 (out of possible 15)

This experience suggests a number of lessons learned.

Purely advisory recommendations can have substantial impact. While the recommendations are sometimes disparaged as purely advisory, they have become the *de facto* international standard. A variety of countries have in fact changed their physical protection practices because more secure arrangements were recommended in the latest revision of INFCIRC/225. Developed countries using nuclear technology typically do want to be seen as laggards in any aspect of technology, safety, or security and take recommendations from the IAEA as defining the acceptable level of effort on nuclear security. And as noted above, many are required by supplier agreements to follow the INFCIRC/225 recommendations, at least for material they received from abroad.

Discussions among technical experts on physical protection lead to more specifics. While most negotiators for the physical protection convention and its amendment were foreign ministry representatives, most of those taking part in discussions of INFCIRC/225 have been technical people who have actually worked on physical protection systems. They have tended to be willing to engage with each other on the technical specifics of physical protection systems and to have a certain professional respect for each other, leading to more rapid agreement on recommendations that were much more detailed.

---

[93] See discussion in Bonnie Jenkins, "Establishing International Standards for Physical Protection of Nuclear Material," *Nonproliferation Review* 5, no. 3 (Spring-Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/jenkin53.pdf as of 19 July 2005).

Measures that are not mandatory may be easier to negotiate. Part of the reason for the rapid negotiation of more specific provisions in the several revisions of INFCIRC/225 may be precisely because states did not *have* to comply with the measures the experts agreed to recommend. Because any state could always say "we do not believe implementing that particular recommendation makes sense," the participants in the discussion likely felt more freedom to agree to specific measures without digging in their heels on each one they might not fully support.

Differing national approaches and levels of priority still limit what can be agreed. It is clear that the widely varying national approaches – and differing views of how urgent the threat of nuclear theft and terrorism really was – have still limited how far the IAEA recommendations could go, leaving them still often focused on a least common denominator. The issue of armed guards for weapons-usable nuclear material is a case in point. In tests in the United States, well-planned outsider attacks on nuclear facilities sometimes move so quickly that there is no time for outside response forces to arrive: armed guards on-site are essential to hold off the attackers until more capable response forces can get to the scene. But some countries argue that on-site armed guards are not necessary. Japan, in particular, has argued vociferously over the years that armed guards on-site are not needed if other protection measures are taken. INFCIRC/225/Rev. 4 compromises on this issue, recommending that sites have guard forces and that if the sites have no armed guards, "compensating measures" should be taken.

International Peer Reviews

In the area of nuclear safety, as opposed to security, international peer reviews – organized by both the IAEA and the World Association of Nuclear Operators (WANO) – have become a commonplace part of doing business in the nuclear industry. International peer reviews of security arrangements are far more problematic, because in most countries, the specifics of nuclear security arrangements are secret. (As noted above, the idea of requiring such international peer reviews, even if only for civilian facilities, was rejected out of hand by the negotiators of the amendment to the physical protection convention.)

Nonetheless, in 1996, the IAEA established the International Physical Protection Advisory Service (IPPAS).[94] IPPAS reviews are purely voluntary; they occur only when a state asks the IAEA for a review. In most cases, IPPAS reviews have been requested by countries in transition from communist economies, or developing countries, who were aware that they needed help with physical protection. In 2003, Norway became the first developed country to host an IPPAS mission, and Norway subsequently indicated that the results of the

[94] For a useful description of IPPAS from a key participant, see Mark Soo Hoo, " IAEA Activities for the Physical Protection of Nuclear Material and Facilities -- the Role and Importance of IPPAS Missions," in *Eurosafe 2002, Berlin, 4-5 November 2002* (Berlin: Forum for Nuclear Safety, 2002; available at http://www.eurosafe-forum.org/products/data/5/pe_253_24_1_euro2_5_7_iaea_phys_pro.pdf as of 11 May 2006).

mission were being used to improve nuclear security in Norway and urged all member states to make use of this service.[95]

To date, IPPAS has been based on comparing the physical protection measures in place to those recommended in INFCIRC/225; hence the security levels recommended as a result of an IPPAS mission would be no higher than those of INFCIRC/225. An IPPAS review typically consists of a team of several physical protection experts from different countries, who might spend a week in a particular country, reviewing physical protection laws and regulations and the actual security measures in place at one or more facilities in the country. The team then prepares a report to the state that requested the review, often suggesting various improvements. These reports are confidential and are not distributed.

The IAEA has no funds for actually carrying out upgrades of nuclear security hardware at the reviewed sites, and often the requesting states do not have funds available either. Hence, following IPPAS missions, the IAEA often works with donor states to attempt to arrange funding for implementing the recommended improvements. In many cases, some of the experts on an IPPAS review team are from donor states and can make the case directly to their governments for paying for the improvements the team recommended. Unfortunately, because the IAEA's role typically ends once a donor state gets involved in implementing the recommended upgrades, the IAEA does not have complete data on how many IPPAS missions have in fact resulted in substantial security upgrades being performed.[96] Nevertheless, it seems clear, for example, that a significant number of the sites where the United States has sponsored security upgrades in the former Soviet Union and at research reactors in other countries had been the subject of IPPAS missions before the upgrades began. Overall, however, in the decade since IPPAS began, there are probably fewer than 20 sites with Category I quantities of weapons-usable nuclear materials where IPPAS missions have led to implementation of substantial security upgrades.[97]

After the 9/11 attacks, with the establishment of the Office of Nuclear Security and the Nuclear Security Fund at the IAEA, resources became available to do more IPPAS missions. The IAEA also added other types of international reviews. Now, the most common IAEA-led reviews are International Nuclear Security Advisory Service (INSServ) missions, which are much broader (but shallower) reviews of all aspects of nuclear and radiological security, ranging from physical protection to capabilities to detect illicit trafficking in radioactive materials at borders; these are, in effect, preliminary needs assessments, which might conclude that physical protection at a particular facility required a more detailed IPPAS-type

---

[95] Government of Norway, "Statement by Norway," in *48th IAEA General Conference, Vienna, Austria, 20-21 September 2004* (Vienna: International Atomic Energy Agency, 2004; available at http://www.iaea.org/About/Policy/GC/GC48/Statements/norway.pdf as of 10 May 2006).

[96] Interview with Anita Nilsson and Richard Hoskins, IAEA Office of Nuclear Security, September 2005.

[97] Even if 100% of the 10 sites with weapons-usable material in the non-Russian states of the former Soviet Union are included, an all seven of the HEU-fueled research reactors where the United States has sponsored upgrades outside the former Soviet Union are added, this comes to 17 sites. There are likely to be few, if any, sites where substantial upgrades were implemented as a result of IPPAS missions where the United States was not involved in some way.

assessment.[98] By the end of 2004, it appears that just under 30 IPPAS missions had been conducted, in over 20 countries, all but Norway being transition countries or in the developing world.[99] Since IPPAS missions cover protection from sabotage as well as theft of nuclear material, by no means all of the countries where IPPAS missions have taken place are countries with weapons-usable nuclear material.

To date, there is no industry organization providing industry-led peer reviews of nuclear security and sharing of best practices in security, as WANO does in the area of safety. This international peer review approach gets mixed reviews using the criteria described above.

Speed: 4

Typically an IPPAS mission is implemented within a year or less of when it is first requested; when the team recommends significant upgrades and the requesting state and a donor state are both willing, these have in some cases been implemented in 2-3 years after the review. But IPPAS has so far only been able to address a few countries, with only a few sites, per year; at that rate, it would take an extremely long time to review and recommend upgrades for all of the most vulnerable nuclear sites worldwide.

Security Level: 3

Because IPPAS recommendations are based on INFCIRC/225, the security level achieved, if the IPPAS mission and subsequent upgrades are successful, should be the same as that achieved by compliance with INFCIRC/225. Since INFCIRC/225 is quite general and does not specify any particular design basis threat that facilities should be defended against, many facilities may still be vulnerable to capable outside attacking groups, or to theft by 1-2 well-placed insiders, even after upgrades are accomplished.

Breadth of Applicability: 2

As noted above, IPPAS reviews are limited to those countries that request them, and a relatively modest number of countries have done so to date. (INSServ missions have been more widely requested, since a much larger number of countries need to address issues related to border controls, control of radioactive sources, and the like, than need to address security for weapons-usable nuclear materials.) It is extremely unlikely that any state will request a peer review of security at a military site (unless circumstances radically change). It would be desirable for a wide range of developed states to request IPPAS reviews of their physical protection arrangements, at least at civilian facilities, making security peer review a normal, regular part of the nuclear business, as safety peer reviews are. This does not appear to be likely in the near term, however, despite Norway's good example.

Summed Effectiveness Rating: 9 (out of possible 15)

---

[98] For a discussion of the INSServ and IPPAS missions conducted in 2004, see International Atomic Energy Agency, *Annual Report 2004* (Vienna: IAEA, 2005; available at http://www.iaea.org/Publications/Reports/Anrep2004/anrep2004_full.pdf as of 3 January 2007), p. 54.

[99] Data compiled from IAEA Annual Reports. Data for 2005 had not yet been published as of spring 2006.

This experience suggests a number of lessons learned.

Secrecy and confidentiality concerns can be overcome enough to allow useful international peer reviews of security. While many states are concerned about keeping their nuclear security approaches secret, a significant number of other states have hosted IPPAS reviews without noticeable ill effect. IPPAS has established a reputation for discretion and for keeping security information confidential. The IAEA has long had procedures for handling confidential safeguards information and has established strengthened procedures for handling security information that could be helpful to terrorists if made public. All states could host IPPAS reviews at least of physical protection for civilian nuclear activities without compromising information that must genuinely remain secret.

Linking reviews to the likelihood of funding for implementing their recommendations is important. Although the IAEA has no funding to implement upgrades recommended by IPPAS reviews, it is clear that many of the countries which have requested IPPAS missions did so in the hope that such a review would be the first step toward receiving assistance to improve their physical protection arrangements. The perception that funding to implement IPPAS recommendations is likely to be available is an important part of IPPAS' effectiveness.

Additional means to convince states to accept IPPAS missions are needed if the effort is to have broader impact. To date, neither developed countries (except Norway) nor countries with military nuclear materials (e.g., Russia, China, India, Pakistan) have been interested in accepting IPPAS missions. The point the Norwegian experience makes is that everyone, not just countries that "need help," can benefit from independent review and advice by international experts. With UNSC 1540's creation of a binding obligation on all states to provide effective security, there would be a justification for pressuring states around the world to accept IPPAS reviews, at least of non-sensitive civilian facilities. Those states that also have military nuclear activities could, as they chose, make use of the approaches suggested during reviews of their civilian activities to improve security for their military activities as well.

International Training and Guidance

In addition to peer reviews, the IAEA offers a wide range of training courses and guidance documents related to nuclear security. This approach began with the International Training Course, focusing on the design and evaluation of physical protection systems, offered every year or two at Sandia National Laboratories since 1978. Similar courses have now been offered in several locations around the world. Other courses that are now being offered range from a workshop on development of a national design basis threat for use in setting nuclear security regulations to a course on operational use of physical protection systems. (The IAEA also provides courses on later lines of defense, such as on radiation detection at borders, and on control of radiological sources.) The IAEA has published or is developing a wide range of guidance documents on physical protection issues, from a detailed handbook on how to implement INFCIRC/225 to guidelines still in development on strengthening nuclear security culture. Indeed, the IAEA now plans a "Nuclear Security

Series" of publications, paralleling the "Nuclear Safety Series" that have become, in essence, the global standards for good practice in nuclear safety.[100]

It is difficult to assess the impact of these training courses and guidance documents on actual nuclear security levels at sites around the world. There is anecdotal evidence that the impact has been significant. Many of those in charge of designing or regulating nuclear physical protection systems in different countries have, at one time or another, been students in the Sandia course or related courses elsewhere in the world. Some of them have indicated that these courses significantly affected their careers in physical protection and their thinking about how best to design a nuclear security system.[101] Experts in many countries look to the IAEA for guidance on nuclear security matters. But tracing back the recommendation in a particular guidance document, or a particular participant in a training course, to specific improvements in physical protection in a particular country, is a very difficult task.

Speed: Unknown

In some cases, a participant in an international training course may return to his or her home country and be asked to design a new physical protection system for a site shortly after participating. Similarly, in some cases countries have essentially developed their regulatory design basis threat during the course of the IAEA workshop on how to do so, or shortly thereafter, and this may have resulted in significant upgrades of their physical protection systems within a year or two thereafter. In other cases, it may take years to draft a guidance document or prepare a course, and it may be many years after the guidance document is issued or the course offered that some aspect of it is taken up and implemented in a particular country.

Security Level: 3

None of the IAEA guidance documents go beyond the INFCIRC/225 recommendations, so one would not expect that the security levels achieved by use of the guidance documents or training courses would be noticeably higher than those achieved by compliance with INFCIRC/225. On the other hand, the design basis threat workshop encourages countries to think through what threats really exist in their country; it may lead to some countries requiring nuclear facilities to be defended against threats substantial enough that they will have to have nuclear security systems going far beyond the requirements of INFCIRC/225.

Breadth of Applicability: Unknown

No one knows exactly how many nuclear facilities in how many countries have security measures in place that are noticeably better than they would be if these training courses and guidance documents had not been provided, nor how many facilities might be affected by these efforts in the future. It seems likely, however, that many states have implemented at least some improved security measures as a result of these training courses and guidance documents.

---

[100] Interview with Anita Nilsson, director of the IAEA Office of Nuclear Security, September 2005.
[101] Interview with John Matter, Sandia National Laboratory, July 2003.

Summed Effectiveness Rating: Unknown

It is difficult to draw lessons from this experience, because so little is known about how effective these guidance documents and training programs are in improving nuclear security around the world. From anecdotal evidence from participants, however, it seems clear that these efforts are well worth their very modest cost. The design basis threat workshops, which help countries put in place a regulatory design basis threat that all their key nuclear facilities must be prepared to defend against, may have particularly large impacts; the creation of such a regulatory design basis threat in the 1970s had a major impact on improving nuclear security in the United States.

Supplier Requirements

Remarkably, for many years the United States exported large quantities of HEU with absolutely no requirements that it be protected from theft. The United States began requiring that recipient states maintain acceptable levels of security for U.S.-origin HEU in the mid-1970s. It appears that West Germany may have been the first state to host a U.S. team to review the adequacy of its physical protection arrangements before approval of a large U.S. export.[102] Also in the mid-1970s, with the formation of the Nuclear Suppliers Group (NSG), the United States convinced the other major suppliers to require at least a minimum level of physical protection for nuclear materials and technologies they exported.[103] In 1978, the requirement that recipient states agree to maintain effective security for U.S.-origin material was written into law, in the Nuclear Nonproliferation Act of 1978.

These supplier requirements have never been especially stringent. The United States requires recipients to protect U.S.-origin material in a manner consistent with the IAEA recommendations. The NSG guidelines only require that Category I material be in a building with a fence around it, under constant watch by guards who are in communication with response forces, to which access is limited to people who have been determined to be trustworthy.[104] The NSG guidelines describe the IAEA recommendations as a "useful basis for guiding" physical protection efforts in recipient states. Despite the many efforts in different states to improve nuclear security since the 9/11 attacks and despite a variety of

---

[102] This review is described in an April 1975 Commerce Department document reviewing the then-planned shipment of HEU to Germany, reproduced in U.S. Senate, *Peaceful Nuclear Exports*, p. 689. The Commerce Department report describes the policy of requiring adequate security for HEU in recipient states as "recently instituted." It indicates that the review concluded that German physical protection arrangements were comparable to those required in the United States at that time.

[103] See the NSG guidelines: International Atomic Energy Agency, *Communications Received from Certain Member States Regarding Guidelines for the Export of Nuclear Material, Equipment and Technology*, INFCIRC/254/Rev. 7/Part 1 (Vienna: IAEA, 2005; available at http://www.nuclearsuppliersgroup.org/PDF/infcirc254r7p1-050223.pdf as of 20 July 2005). For a discussion of these legal requirements and other legal agreements in which some states have committed to comply with the IAEA recommendations, at least for particular designated stocks of material, see Jenkins, "Establishing International Standards for Physical Protection of Nuclear Material."

[104] International Atomic Energy Agency, *INFCIRC/254.*

ongoing efforts to revise the NSG guidelines, there appears to have been no effort to make either U.S. or NSG physical protection requirements more stringent since the 9/11 attacks.

The United States makes a modest effort to check that countries are complying with their commitments to provide effective security (as required by U.S. law). Small U.S. teams occasionally visit recipient states to check on this but this effort is very small: prior to 9/11, only one to two such visits typically took place per year, meaning that it would be many years, on average, between one visit to a particular country and the next. The teams do not have the resources to perform real vulnerability assessments at the sites they visit; instead, they check off the requirements of the IAEA's recommendations.[105] It is not clear whether any of the other suppliers perform similar checks.

Many countries that have been subject to these supplier requirements are also leading countries which do not want to be seen as laggards in either nuclear safety or nuclear security. It is difficult to determine whether their actions to comply with the IAEA recommendations would have occurred regardless of supplier requirements, or were driven by the legal requirement to comply with their supply agreements. Hence, it is difficult to determine how much independent effect these supply conditions have had.

Speed: Unknown

No data is publicly available concerning how rapidly, after the policy of requiring nuclear security consistent with IAEA recommendations as a condition of supply was adopted, countries changed their physical protection arrangements to come into compliance.

Security Level: 3

Since the level of security the United States has required has been consistency with IAEA recommendations, the security level rating is the same as that given those recommendations.

Breadth of Applicability: 3

A substantial fraction of the civilian nuclear material worldwide is subject either to the U.S. requirement or to requirements from other supplier states party to the NSG guidelines. Military material and civilian material not supplied by NSG members, however, is not subject to these requirements.

Summed Effectiveness Rating: Unknown

A number of lessons can be drawn from this experience.

Many states are willing to legally commit to minimum levels of physical protection if doing so is part of receiving technology and material from leading suppliers. A remarkable number of states have been willing to commit to follow the IAEA recommendations in negotiating nuclear supply agreements with the United States – and to accept U.S. reviews of physical protection arrangements – even though many of the same states vociferously rejected requirements to comply with the IAEA recommendations and accept peer reviews in negotiations over the physical protection convention and its recent

[105] Interview with DOE official, April 2002.

amendment. This suggests that the sovereignty barrier to agreeing on effective international nuclear security standards is not absolute, but depends on the incentives offered in the negotiation.

Most suppliers put low priority on ensuring effective security for the material they supply. It is remarkable that the NSG agreed in 1975 on physical protection requirements so much less specific than the IAEA guidelines and has not seriously considered toughening those requirements in the three decades since. Most suppliers appear to make little effort to ensure that recipients have effective security measures in place. Even the United States, which has the toughest supplier requirements in this area and does do some limited checks to ensure that states are complying with those requirements, has given the effort to ensure security for U.S.-supplied material quite low priority over the years, except at moments when security for these materials became a political issue (as occurred when separated plutonium from reprocessing began being shipped from Europe to Japan, for example, and again in recent years when U.S. weapons-grade plutonium was shipped to France for fabrication into lead test assemblies of plutonium-uranium mixed oxide (MOX) fuel).

Technical Cooperation

As the Soviet Union teetered toward collapse in 1991, the U.S. Congress approved the Nunn-Lugar initiative, authorizing $400 million to assist in dismantling Soviet weapons and preventing their proliferation. Over the 15 years since, cooperative threat reduction has grown into a sprawling enterprise addressing many different types of threats, with U.S. expenditures totaling over $1 billion per year, nearly matched by other participants in the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction, announced at the 2002 summit of the Group of Eight industrialized democracies.

As part of this enterprise, the United States has worked with Russia and the other states of the former Soviet Union to install modern security and accounting systems for both nuclear warheads and weapons-usable nuclear materials. Other donor states have taken part as well, though on a much smaller scale. Building this cooperation has required overcoming immense obstacles, from secrecy and distrust to unwieldy contracting procedures.[106] For a period, laboratory-to-laboratory cooperation, with only limited oversight and interference from central government officials, proved remarkably successful, with technical people empowered to work directly with their colleagues at individual sites, offering respect, money, and interesting work that clearly served both countries' security interests, building trust step-by step. The Russian participants were highly motivated to move the cooperation forward and pushed for approval within their own government in ways the Americans could not. This worked far better, in many cases, than government-to-government talks in which mid-level officials – none of whom would benefit directly from upgrades and each of whom faced

[106] For discussions of this history, see, for example, Bunn, "Cooperation to Secure Nuclear Stockpiles"; Caitlin Talmadge, "Striking a Balance: The Lessons of U.S.-Russian Materials Security Cooperation," *Nonproliferation Review* 12, no. 1 (March 2005; available at http://cns.miis.edu/pubs/npr/vol12/121/121talmadge.pdf as of 2 November 2005); Bukharin, Bunn, and Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union.*

significant career risks if the work proved to compromise secrets or lead to the diversion of funds – sought to negotiate overall agreements at headquarters before any work was done.

Today, although there is much left to do, nuclear security in the former Soviet Union is very noticeably improved: it would be surprising if there is any facility remaining that is not protected against the kinds of thefts that occurred in the mid-1990s – a single insider pocketing material without being noticed, or a single outsider walking through a gaping hole in a fence, stealing material, and retracing his steps without setting off any alarm.[107] Security and accounting upgrades have been completed at all the facilities with weapons-usable nuclear material in the non-Russian states of the former Soviet Union (though whether these upgrades are sufficient to meet the threats that exist in these countries and whether they will be sustained as U.S. assistance ends remain critical questions). As of the end of fiscal year (FY) 2005, U.S. and Russian experts have completed all planned security and accounting upgrades for 54% of the buildings in Russia where weapons-usable nuclear materials are located (and an initial suite of rapid upgrades for another 23%); similar upgrades have been completed for some 45% of the sites where nuclear warheads are located in Russia.[108] Following a summit accord on nuclear security between President George W. Bush and Russian President Vladimir Putin in Bratislava in February 2005, progress has accelerated noticeably, and the two sides have agreed on a joint plan to complete upgrades at all but a few nuclear material sites (and most nuclear warhead sites) by the end of 2008.

The United States and some other donor states have also pursued technical cooperation to upgrade security in several other states, as noted above. The United States and China began a lab-to-lab cooperation on nuclear security and accounting in the 1990s, but this foundered amid mutual accusations of nuclear spying.[109] U.S.-Chinese nuclear security cooperation recently restarted, and a modern security and accounting system had been installed at one civilian site with Category I nuclear material in China by the end of 2005. India has not yet agreed to nuclear security cooperation with the United States, though it has sponsored IAEA regional workshops on nuclear security issues in India. There have been some public reports suggesting that Pakistan and the United States are cooperating to some degree on nuclear security, but no official information is available.[110] Security upgrades have been completed for several HEU-fueled research reactors in Eastern Europe and for facilities in Portugal and Greece. Such upgrades are planned for several more facilities as part of DOE's Global Threat Reduction Initiative (GTRI).[111]

---

[107] For a recent discussion, see Matthew Bunn and Anthony Wier, *Securing the Bomb 2006* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2006; available at http://www.nti.org/securingthebomb as of 23 July 2006).

[108] See discussion and references in Bunn and Wier, *Securing the Bomb 2006*.

[109] Nancy Prindle, "The U.S.-China Lab-to-Lab Technical Exchange Program," *Nonproliferation Review* 5, no. 3 (Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/prindl53.pdf as of 11 May 2006).

[110] Kenneth N. Luongo and Isabelle Williams, "Seizing the Moment: Using the U.S.-Indian Nuclear Deal to Improve Fissile Material Security," *Arms Control Today* (May 2006; available at http://www.armscontrol.org/act/2006_05/usindiafissilesecurity.asp as of 12 May 2006).

[111] Data provided by DOE, December 2005.

This cooperation gets higher ratings than some of the other approaches, using the three criteria outlined earlier.

Speed: 3

The speed of such technical cooperation has varied, in different parts of the program at different times. When there is political agreement and the pace is limited only by what the technical experts can get done, comprehensive upgrades for an entire site have in some cases been implemented within 18 months of the beginning of work. But at many sites, a variety of bureaucratic obstacles and other problems have delayed the work for years at a time, with the result that after a dozen years of work, the full set of needed upgrades is completed at only modestly more than half of the buildings with weapons-usable nuclear material in Russia.[112]

Security Level: 4

Currently, cooperative upgrades in Russia are being designed to provide protection against a significant group of well-armed and well-trained outside attackers or one to two insiders, or both working together – a substantially higher security level than required by the IAEA recommendations (though less than the post-9/11 design basis threat DOE facilities are required to defend against). Whether corruption and lack of security culture among the guards and staff at some sites will undermine security even after modern equipment is in place remains an open question, however. Whether high levels of security will be sustained after U.S. and international assistance comes to an end remains an equally difficult question.

Breadth of Applicability: 4

After years of negotiation, U.S. and Russian experts are working together throughout Russia's nuclear weapons complex, its civilian nuclear complex, its naval complex, and at many of Russia's nuclear warhead facilities. The two remaining nuclear warhead assembly/disassembly facilities are the main nuclear material sites that are still off-limits to cooperation. In principle at least, some of the approaches developed in Russia – with modifications to address the even greater secrecy barriers in some other countries, cultural differences, and other issues – could be applied for a large fraction of the world's nuclear stockpiles. In the cases of high-income developed countries, cooperation would be more likely to take the form of technical interchange than U.S.-funded assistance.

Summed Effectiveness Rating: 11

As efforts to improve nuclear security worldwide move forward, lessons should be drawn from the experience in Russia – though the approaches developed in this cooperation in Russia will have to be modified substantially to succeed in other contexts where the United States is now pursuing nuclear security cooperation, from China to India and Pakistan. Four lessons from U.S.-Russian nuclear security cooperation over the last 15 years will be crucial to success.[113]

Top-down, bottom-up, but not middle-through. The effect of the Bratislava summit demonstrates that presidential leadership can have a major effect in breaking through

[112] See discussion in Bunn and Wier, *Securing the Bomb 2006.*

[113] This discussion is drawn from Bunn, "Cooperation to Secure Nuclear Stockpiles."

obstacles to nuclear security cooperation. Presidential initiatives are particularly effective when powerful and motivated actors are assigned to follow through. As the remarkably successful experience with U.S.-Russian laboratory-to-laboratory cooperation lab-to-lab experience shows, bottom-up initiatives starting with technical experts at individual sites can also be remarkably powerful, if they remain beneath the radar of officials who may be motivated to put obstacles in their path. Mid-level nuclear officials, by contrast, usually have little flexibility to introduce major changes in approaches to nuclear security and usually resist foreign attempts to convince them to do so. The bottom-up approach, however, is more likely to work in countries undergoing revolutionary transformation, as Russia was in 1992, or in more stable countries where the necessary work is modest in scale and not especially sensitive (such as upgrading security or converting the fuel at a single HEU-fueled research reactor, the only nuclear facility of concern in many countries), or where cooperation at sensitive nuclear installations has a public imprimatur from the highest levels.

In general, the experience of the past 15 years suggest that innovations in nuclear security are most likely to be successful when they are driven forward by a small group of committed and well-connected individuals who are able to take advantage of events that create a sense of urgency (as in the cases of the collapse of the Soviet Union in 1991 and the nuclear material seizures in 1993-1994). Such small groups are able to maintain substantial creativity and flexibility in their approaches and to build trust with foreign partners. Innovations are most likely to be blocked, slowed, or overturned when large numbers of officials and agencies become involved, many of whom may be committed to past approaches or may not see the advantages of new ones.

Partnership works. As the lab-to-lab effort (and the nuclear security cooperation with the Russian Navy that followed it) show, cooperation on nuclear security is most effective when it incorporates ideas and resources from both sides. Countries such as China, India, and Pakistan are far more likely to join an effort framed as a partnership of the leading nuclear states to ensure nuclear security worldwide than one described as assistance to countries too weak and uninformed to take care of nuclear security themselves. Building trust among the participants in such a partnership is crucial to gaining the flexibility needed to overcome the inevitable obstacles. Despite the urgency of the problem, in some cases it is necessary to start with small projects to build trust before expanding to more substantial efforts. It is also essential to follow through on what has been agreed, rather than ripping up previous agreements. Only when the people who will use and maintain an improved nuclear security system are directly involved in conceiving, designing, and implementing the new approach are they likely to work their own government to overcome obstacles and to use and maintain the new system effectively after foreign assistance comes to an end. This lesson is not unique to nuclear security cooperation: a major World Bank study, for example, pointed out that 62% of rural water projects that promoted extensive participation by the recipients were successful, compared to only 10% that did not.[114]

---

[114] World Bank, *Assessing Aid: What Works, What Doesn't, and Why* (Oxford, United Kingdom: Oxford University Press, 1998). For a useful discussion of the specific differences between partnership-based approaches and donor-recipient approaches, see Albert R. Wight, "Participation, Ownership, and Sustainable

Building commitment and a sense of urgency is crucial. If senior officials and facility managers are to assign sufficient resources to nuclear security and do the political work to change approaches, they must be convinced that the threat of nuclear theft and terrorism is real and urgent. Measures that might be taken include joint threat briefings by senior experts from the United States and the potential partner country; war games and similar simulations of nuclear terrorism scenarios, which engage hearts and minds in a way that paper reports and briefings never do; putting together teams of security experts from potential recipient countries to do rapid assessments of vulnerabilities at their own nuclear facilities (as DOE did for its facilities after the 9/11 attacks); working with countries to help them identify insider and outsider threats their facilities should be defended from (as the IAEA has been working to do in recent years); and producing training videos for facility managers and staff outlining the dangers of nuclear theft and sabotage, including emotional images of Hiroshima and Chernobyl to highlight the potential consequences of nuclear terrorism.[115]

Flexible approaches on secrecy and access are needed. To be successful, security upgrade programs in many cases will have to acknowledge that countries are simply not going to reveal all of their nuclear security secrets. For example, Pakistan is very unlikely to allow U.S. or other foreign experts to visit all its nuclear weapon storage facilities and fully understand their security vulnerabilities; Pakistan is legitimately concerned that the United States might at some time want to destroy or seize control of its nuclear arsenal, or might inadvertently leak secrets to India. India has similar concerns, as does China. But there is a great deal that can be done to improve security for nuclear sites without actually seeing them or learning anything very specific about them – from detailed discussions of techniques and best practices for assessing vulnerabilities to outsider and insider threats, to identifying some of the best commercially available equipment, to training and other help with writing and enforcing effective nuclear security rules. Using methods developed in the lab-to-lab program, the United States or other donor countries can finance security upgrades at sites their experts will never visit, while ensuring that their money is being spent appropriately.

Material Removals

Improved security arrangements can only reduce, never eliminate, the risk that nuclear material will be stolen from a particular site. The risk of nuclear theft from a site can be entirely eliminated only by removing the nuclear weapons or weapons-usable nuclear material from that site, so that there is nothing left to steal. Moreover, if the number of sites to be protected can be reduced, higher security levels can be purchased at lower total cost. Hence, efforts to convince sites around the world to abandon the use of weapons-usable nuclear material and allow the material at their sites to be removed are another key policy tool for strengthening the global nuclear security system.

Development," in *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries*, ed. Merilee S. Grindle (Cambridge, Mass.: Harvard University Press, 1997).

[115] For a discussion of such measures, focused primarily on their potential use in Russia, see Bunn and Wier, *Securing the Bomb 2005*, pp. 96-97.

Such efforts began in earnest in 1978, with the launch of the Reduced Enrichment for Research and Test Reactors (RERTR) program, whose goal has been to convert as many as possible of the world's HEU-fueled research reactors to use LEU instead. By late 2005, 32 reactors had fully converted to the use of LEU fuel (with 10 more in the process of conversion), and DOE was hoping to convert the remaining 74 reactors on its target list of 106 facilities by the end of 2014.[116] Unfortunately, however, DOE's list excludes nearly half of the HEU-fueled reactors currently operating in the world, which are judged to be too difficult to convert to LEU, for one reason or another (some, for example, are fast reactors, which would have difficulty achieving criticality with LEU).[117] Moreover, over the years it has become clear that many reactor operators are reluctant to convert to LEU, and substantial incentives are required to convince them to do so. Under a U.S. law known as the Schumer amendment, passed in 1992, U.S. HEU can only be exported to research reactors that (a) cannot use existing LEU fuels, and (b) commit to convert to LEU as soon as suitable fuels become available. Similarly, the U.S. offer to take back irradiated U.S.-origin research reactor fuel excludes reactors that could convert to LEU but refuse to do so. These steps have given those reactors that need regular supplies of fresh fuel and need a place to send their irradiated fuel strong incentives to agree to convert. But for reactors that have other supplies of fresh fuel and other plans for their irradiated fuel, along with reactors that fuel cores that will last for many years or for the lifetime of their facilities, there are few incentives to convert to LEU.

The U.S. take-back offer, renewed in 1996, represents a complementary effort to reduce the number of sites around the world where poorly protected HEU continues to exist. Unfortunately, however, to date the offer does not cover some two-thirds of the U.S.-supplied HEU abroad (because the 1996 renewal was limited only to types of material the United States had facilities ready to process), and only about half of the material that is covered is expected to be returned, unless stronger incentives are put in place to convince facilities to take advantage of the offer.[118] In any case, after a 2005 extension of the deadline for the take-

---

[116] Christopher Landers, "Reactors Identified for Conversion: Reduced Enrichment for Research and Test Reactors (RERTR) Program," in *RERTR 2005: 27th International Meeting on Reduced Enrichment for Research and Test Reactors, Boston, Mass., 6-10 November* (Argonne, Ill.: Argonne National Laboratory, 2005; available at http://www.rertr.anl.gov/RERTR27/PDF/S9-1_Landers.pdf as of 20 June 2006). For useful recent overviews of efforts to remove HEU from reactor sites around the world, see Frank von Hippel, "A Comprehensive Approach to Elimination of Highly-Enriched Uranium from All Nuclear Reactor-Reactor Fuel Cycles," *Science and Global Security* 12, no. 3 (November 2004); Alexander Glaser and Frank N. Von Hippel, "Thwarting Nuclear Terrorism," *Scientific American* 294, no. 2 (February 2006).

[117] Data compiled by Frank von Hippel and Alexander Glaser of Princeton University. Frank von Hippel, personal communication, December 2005.

[118] U.S. Department of Energy, Office of the Inspector General, *Audit Report: Recovery of Highly Enriched Uranium Provided to Foreign Countries*, DOE/IG-0638 (Washington, D.C.: DOE OIG, 2004; available at http://www.ig.doe.gov/pdf/ig-0638.pdf as of 3 March 2005); U.S. Congress, Government Accountability Office, *Nuclear Nonproliferation: DOE Needs to Consider Options to Accelerate the Return of Weapons-Usable Uranium from Other Countries to the United States and Russia*, GAO-05-57 (Washington, D.C.: GAO, 2004; available at http://www.gao.gov/new.items/d0557.pdf as of 2 February 2005).

back, this take-back effort is not expected to be completed until 2019.[119] In recent years, the United States and Russia have been cooperating on similar efforts to convert Soviet-supplied research reactors to LEU and to return Soviet-supplied HEU to Russia (or blend it to LEU outside of Russia).

In 2004, all of these reactor conversion and take-back efforts were consolidated in the Global Threat Reduction Initiative, which was given a mission to accelerate and strengthen efforts to remove weapons-usable nuclear material from vulnerable sites around the world.[120] HEU has been removed from several Soviet-supplied sites in the last several years. In the aftermath of the Bush-Putin Bratislava summit in 2005, Russia and the United States agreed on a schedule for returning Soviet-supplied HEU to Russia by the end of 2010.[121] DOE expects, however, that some countries with Soviet-supplied HEU will prefer to use it as reactor fuel or blend it down outside of Russia, rather than sending it back in the near term, and these steps may take longer.[122] As a result, DOE does not expect to complete its efforts to eliminate these Soviet-supplied HEU stockpiles until 2013.[123] In this case, too, DOE is finding that some facilities are quite reluctant to give up their HEU and that substantial incentives may be needed to convince them to do so.

Before the launch of GTRI, there had also been several ad-hoc efforts to remove HEU from vulnerable sites, including Project Sapphire (which air-lifted some 580 kilograms of HEU from the Ulba fuel facility in Ust-Kamenogorsk, Kazakhstan, to the United States); Operation Auburn Endeavor (which airlifted several kilograms of HEU from a small research facility in Tbilisi, Georgia, to the British reprocessing facility at Dounreay in 1998); and Project Vinca (which airlifted 48 kilograms of HEU from the Vinca Institute of Nuclear Sciences near Belgrade to Russia in 2002). Although each of these was considered urgent, for security reasons, each took years to organize, and each required a different package of incentives to close the deal. Indeed, in the case of Project Vinca, the U.S. government concluded that none of its agencies had the authority or funding to offer to pay for managing the institute's spent fuel, which was the Yugoslav price for sending away the fresh HEU at the

---

[119] U.S. Department of Energy, *FY 2007 Congressional Budget Request: National Nuclear Security Administration--Defense Nuclear Nonproliferation*, vol. 1, DOE/CF-002 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_1_NNSA.pdf as of 3 January 2007), p. 562.

[120] Spencer Abraham, "International Atomic Energy Agency, Vienna: Remarks Prepared for Energy Secretary Spencer Abraham" (Washington, D.C.: U.S. Department of Energy, 26 May 2004; available at http://www.energy.gov/news/1800.htm as of 12 May 2006). Several colleagues and I had been pressing for the establishment of such a program for years, and administration officials have indicated privately that these recommendations were influential in the establishment of GTRI. For an early proposal, see Matthew Bunn, John Holdren, and Anthony Wier, *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/securing_nuclear_weapons_and_materials_May2002.pdf as of 2 January 2007).

[121] "Statement on Nuclear Security Cooperation with Russia" (Washington, D.C.: The White House, Office of the Press Secretary, 30 June 2005; available at http://www.whitehouse.gov/news/releases/2005/06/20050630-4.html as of 7 July 2005).

[122] Interview with DOE officials, December 2005.

[123] U.S. Department of Energy, *FY 2007 Defense Nuclear Nonproliferation Budget Request*, p. 562.

site, and the private Nuclear Threat Initiative (NTI) had to step in with a $5 million commitment. This experience helped drive the decision to establish the Global Threat Reduction Initiative.[124]

Individual states have also taken steps to consolidate their nuclear stockpiles. In the United States, for example, the number of private facilities with weapons-usable nuclear material has declined dramatically since the 1970s, in part because the cost of meeting new security requirements for such material created an incentive to get rid of it. The Department of Energy has consolidated its nuclear material holdings in fewer buildings at some sites and has closed other major sites entirely (such as Rocky Flats), saving hundreds of millions of dollars a year in safety and security costs. DOE is continuing its effort to consolidate its stocks.[125] In Russia, the number of nuclear warhead facilities has been reduced substantially with the pull-back of nuclear weapons from Eastern Europe and the non-Russian states of the former Soviet Union and the large-scale removal of tactical weapons from front-line deployments that accompanied the Bush-Gorbachev nuclear initiatives of 1991-1992.[126] But the number of nuclear warhead sites is still far larger than seems necessary for post-Cold War nuclear needs, and Russia appears to have had little interest in planning and implementing a large-scale consolidation of weapons-usable nuclear materials. (U.S. efforts to convince Russia to remove material entirely from some sites as part of the Material Consolidation and Conversion sub-program have run into strong resistance.)

This complex of approaches receives mixed ratings using the criteria above.

Speed: 2-4

Different parts of the material removal effort have moved at different speeds. The pace of reactor conversion has been glacially slow, amounting to just over one reactor converted per year in the nearly three decades since the effort began; while DOE now plans to accelerate that pace dramatically, to meet its goal of converting 74 more reactors by 2014, whether it will succeed remains an open question. The ad-hoc efforts to remove material from particular vulnerable sites seemed painfully slow given participants' fears that the material would be stolen before it was removed, but most of these efforts did succeed in getting material removed within a couple of years of when the initiative began in earnest – and it appears this pace is accelerating with the more focused, less ad-hoc approach being taken in GTRI.

---

[124] For a useful discussion of these cases, see Philipp C. Bleek, *Global Cleanout: An Emerging Approach to the Civil Nuclear Material Threat* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2004; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/bleekglobalcleanout.pdf as of 13 April 2005).

[125] For a far-reaching set of non-government proposals for consolidation, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006).

[126] For useful discussions, see Gunnar Arbman and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part II: Technical Issues and Policy Recommendations*, vol. FOI-R—1588—SE (Stockholm: Swedish Defense Research Agency, 2005; available at http://www.foi.se/upload/pdf/FOI-RussiasTacticalNuclearWeapons.pdf as of 12 April 2005); Gunnar Arbman and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part I: Background and Policy Issues*, vol. FOI-R--1057--SE (Stockholm: Swedish Defense Research Agency, 2003).

Security Level: 5

Where the weapons-usable nuclear material is removed entirely, the probability of nuclear theft is reduced to zero.

Breadth of Applicability: 3

While international cooperative efforts to remove weapons-usable nuclear material have been completed at only a modest number of sites to date, they are potentially applicable to a much broader range of facilities. IAEA experts, for example, estimate that of the roughly 270 research reactors operating in the world today (roughly half of which use HEU fuel), only 30-40 are needed for the long term[127] – meaning that 80-90% of the world's research reactors can be shut down and their material removed. Many of the remainder can be converted to LEU. In the United States, Russia, and potentially some other nuclear weapon states, substantial consolidations of military nuclear stockpiles into fewer locations remain feasible and desirable.

Summed Effectiveness Rating: 10-12

A variety of lessons can be drawn from this experience.

Rapid success in material removals requires packages of incentives to convince states and facilities to give up their weapons-usable material. The experience to date suggests that incentive packages are needed that are targeted to the needs of each individual facility. Needed incentives could include: help converting a reactor to LEU; help shutting a facility down and decommissioning it; contracts for the site's scientists to do other research not requiring the weapons-usable material in question; help managing irradiated fuel and radioactive waste at the site; or, in some cases, incentives to motivate the government to cooperate, which may be unrelated to the particular facility in question (as was the case with some of the incentives package provided to Kazakhstan as part of Project Sapphire, for example).[128] Unfortunately, to date GTRI has taken the view that it will provide assistance to reactors to convert to LEU and will seek to ensure that conversion does not make them worse off, but will not fund any incentives that would make them better off as a result of conversion.[129]

Success requires a focused, comprehensive approach, with a comprehensive set of tactics. The establishment of GTRI, pulling together and expanding what had previously been a set of small, stove-piped programs working on pieces of the material-removal problem, has already accelerated the pace of removals. GTRI still needs to expand its approach, however, to cover the full universe of potentially vulnerable materials and reactors, to include offers of targeted incentives, to include shut-down as well as conversion as a policy option,

---

[127] International Atomic Energy Agency, "New Life for Research Reactors? Bright Future but Far Fewer Projected" (Vienna: IAEA, 8 March 2004; available at http://www.iaea.org/NewsCenter/Features/ResearchReactors/reactors20040308.html as of 5 January 2007).

[128] Bleek, *Global Cleanout.*

[129] Interview with DOE officials, December 2005.

and to more regularly call in high-level political leaders when needed to press a particular country to cooperate. [130]

Some Overall Lessons From Past Efforts to Improve Nuclear Security

There are several overarching lessons from the experience with the policy tools just discussed that will be applicable to any near-term effort to improve the performance of the global nuclear security system. First, building the sense of urgency and commitment in other countries is absolutely critical. If other countries do not believe there is a real threat to their own security that needs to be addressed, any attention they devote to nuclear security will be grudging and half-hearted. Second, in most cases mid-level officials are simply not able to overcome the systemic obstacles to agreement on in-depth nuclear security cooperation or stringent nuclear security standards. If a really fast-paced global effort to improve security for nuclear stockpiles or a stringent global nuclear standard are to be put in place, this will have to be done at the highest political levels – and probably in a way that largely bypasses the relevant bureaucracies as was done, for example, in the 1991 Bush-Gorbachev nuclear initiatives (which led to the pull-back and dismantlement of many thousands of nuclear weapons) or, more recently, in the Bush-Singh accord on civil nuclear cooperation with India. Those past accords, along with the results of the Bush-Putin Bratislava summit, make clear that presidential intervention can make a real difference in overcoming apparently systemic obstacles. Third, approaches based on real partnership, demonstrably serving the interests of all parties and incorporating ideas and resources from all parties, are likely to be far more effective than approaches where this sense of partnership is missing. The days when the United States could simply dictate nuclear approaches to other countries are long gone. Fourth, incentives are critical – at the levels of states, of key ministries within those states, of facility managers, and of individuals and teams on the staff of particular sites. As effective nuclear security measures are expensive and often inconvenient, the incentives to cut corners on security are high; strong incentives pointing the other direction are essential to ensuring effective and sustainable security for the world's nuclear stockpiles.

[130] Bunn and Wier, *Securing the Bomb 2006*. GTRI managers have been reluctant to pursue a shut-down agenda out of fear that reactor operators who see them as coming to shut their facility will react negatively and be unwilling to cooperate on conversion to LEU. This is a legitimate concern. It is possible that a shut-down initiative should be pursued separately, perhaps as an IAEA-led "Sound Nuclear Science Initiative," focused on getting the needed nuclear science, testing, training, and isotope production done at the least cost.

6. Conclusions and Recommendations

In this dissertation, I have examined several of the most important elements of the problem of nuclear terrorism:

- How big is the risk?
- How can we assess which nuclear facilities and transport legs are the biggest contributors to this risk?
- What policy tools can be expected to be most effective in improving security at these facilities and transport legs, so as to reduce the risk or nuclear theft and terrorism?

How Big is the Risk of Nuclear Terrorism?

In Chapters 2 and 3, I provided both a qualitative assessment of the risk of nuclear terrorism and a quantitative model for structuring thinking about this risk. The qualitative assessment made clear that:

- Some terrorist groups have actively sought the means to make nuclear bombs;
- It is plausible that a well-organized and sophisticated terrorist group could make a crude nuclear bomb if they got the needed weapons-usable nuclear material;
- World stockpiles include tens of thousands of nuclear weapons possessed by possessed by nine countries (and deployed on the territory of a few more) and many hundreds of tons of weapons-usable nuclear material, which exists in more than forty countries worldwide;
- Security measures currently in place for nuclear weapons and materials vary widely, with some stockpiles very secure and others demonstrably not secure enough to protect against some of the threats that terrorists and criminals have shown that they can pose; and
- There are so many ways to introduce nuclear material or a nuclear bomb across the border of a major state that measures to prevent nuclear smuggling can only make a modest contribution to reducing the overall threat of nuclear theft and terrorism.

At the same time, however, this assessment also indicated that:

- The few terrorist nuclear weapons efforts about which data has become available to date have largely been fairly unsophisticated and do not appear to have achieved an in-depth understanding of the technical subjects that would have to be mastered to build a bomb (though other terrorist groups or cells may, for all we know, have mastered those subjects or be in the process of doing so);
- There is no conclusive evidence that either a nuclear weapon or the materials to make one have yet fallen into the hands of terrorist groups or hostile states;
- Security for many nuclear stockpiles around the world has improved markedly in the years since the 9/11 attacks;

- The spotty evidence available suggests that the difficulty of making connections and closing deals between people in a position to steal nuclear material and potential buyers is a significant obstacle to nuclear terrorism; and
- The overthrow of the Taliban regime that gave al Qaeda sanctuary in Afghanistan and the substantial damage inflicted on the old centrally-controlled al Qaeda since the 9/11 attacks have probably significantly reduced al Qaeda's chances of success in carrying out a complex project like getting a nuclear weapon or weapons-usable material and transforming them into workable nuclear explosive.

In Chapter 3, I presented a mathematical model of the risk of nuclear terrorism, based on assigning estimated probabilities to an event tree of various possible terrorist decisions about how to attempt to get nuclear weapons and the probabilities of success or failure at various steps on those paths. I then discussed the publicly available information that could inform judgments about how large or small each of the key parameters might be. A numerical example of the use of the model, using plausible values for each of the model parameters, resulted in an estimated 29% probability of a terrorist attack using a nuclear explosive somewhere in the world over the next decade, leading to an estimated expected cost over 10 years of over $1 trillion. While this probability estimate is extremely uncertain, even far more optimistic values for key parameters still led to an estimated 8% 10-year probability; reducing the estimated probability to 1% over 10 years would require very optimistic estimates – and would still result in an expected cost of some $40 billion over 10 years.

In short, Chapters 2 and 3 together made a strong case that the risk is big enough to justify a substantial effort to reduce it. No one in their right mind would operate a large nuclear power plant upwind of a major city that had a one-in-a-thousand annual probability of a catastrophic radioactive release; that would correctly bee seen as far too high a risk to be acceptable. Yet the arguments in Chapter 2 and 3 strongly suggest that the way the global nuclear security system is operating today imposes at least this high an annual risk of the destruction of a major city somewhere in the world – and probably a much higher risk.

Chapter 3 strongly suggested that the most effective measures to reduce the risk of nuclear terrorism are those that have their effect early in the event tree – in particular, counterterrorism efforts that reduce the number of plausible nuclear terrorist groups and their effectiveness and improvements in nuclear security that reduce the probability that nuclear material could be successfully stolen. The key advantage of nuclear security efforts, even over counter-terrorism efforts, is that they do not require intelligence breakthroughs: most of the locations where security improvements are needed are well known, as are the technologies and approaches that offer improved security. The key obstacles to be overcome are political, centering around complacency, secrecy, and national sovereignty. Once a nuclear weapon or nuclear material has left the facility or transport leg where it is supposed to be, by contrast, efforts to recover it and prevent it from being used in a terrorist nuclear attack are all variations on looking for needles in haystacks – except that there are intelligent adversaries trying to keep the needles hidden.

A key result in Chapter 3, which was not derived from the model but based on analysis of how large the estimated probability of successful insider and outsider thefts should be in

the model, was that it is not the *average* nuclear security measures in a particular country that are important, but their *distribution* – and in particular whether there are some facilities with particularly weak security measures. In essence, the probability of successful theft is only substantial where the distribution of security levels and the distribution of capabilities thieves can bring to bear overlap – that is, where there is a good chance thieves can pull together a level of capability beyond the level the security system can cope with. Hence, the small portion of facilities and transport legs that are most vulnerable and face the highest threats pose a large fraction of the total risk – both because thieves are more likely to choose to try to steal from them (if they correctly detect these security weaknesses) and because they are more likely to succeed if they do. This suggests that relatively modest investments in improving security (or removing the stockpiles to be stolen) at a few especially vulnerable sites facing especially high threats might lead to a large reduction in overall risk. If, on the other hand, terrorists are able to detect and respond to the increased security levels – for example recruiting additional participants for the theft attempt – the reduction in risk from improving security at the most vulnerable sites would be less.

How Can We Assess Where the Biggest Risks Lie?

In Chapter 4, I laid out a detailed methodology for assessing which nuclear facilities and transport legs posed the greatest risks of nuclear theft. In this approach, the overall risk is assessed by combining the probability of successful theft and the probability that a successful theft would lead to successful bomb-making.

The probability of successful theft is determined by the threat level (that is, the kinds of capabilities thieves are able to bring to bear for a theft attempt in that country) and the security level (that is, the kinds of capabilities the nuclear security system at a particular facility or transport leg are able to defeat). In Chapter 4, I described a wide range of types of capabilities thieves might bring to bear in attempting to steal nuclear weapons or materials and a wide range of information and sources for acquiring it that analysts should make use in making estimates of threat levels and security levels.

The probability of successful bomb-making after a successful nuclear theft is determined by the quantity and quality of the nuclear material stolen, as it relates to the capabilities of the recipients of the material (or the particular safeguards against unauthorized use in place and the quantity and quality of the material contained, in the case of theft of an actual nuclear weapon). In Chapter 4, I assessed the difficulties sub-national adversaries would face in overcoming a wide range of isotopic, chemical, radiological, and other barriers to bomb-making that might be posed by different types of material that might be stolen. Based on these assessments, I assigned "discount factors" – estimated factors by which the probability of successful bomb-making would be reduced by the characteristics of the material, compared to the probability in the case of large quantities of weapon-grade HEU metal – to a wide range of types of material.

A key result from this examination was that current systems for categorizing nuclear materials in use by the U.S. Nuclear Regulatory Commission (NRC), U.S. Department of Energy (DOE), and the International Atomic Energy Agency (IAEA) for the purposes of assigning different levels of security requirements are badly flawed and allow some materials

that potentially might be quite attractive for sub-national bomb-making to have only modest levels of protection. In particular, I argued that many of the systems represented not "graded safeguards" but "cliffed safeguards," in which, once nuclear material reached an essentially arbitrary threshold (such as emitting more than 100 rad per hour at one meter), the protection it was afforded plummeted. I offered an alternative categorization approach based on the discount factors I had developed, the use of which would result in a more genuinely graded approach to physical protection.

I then offered an illustrative example of how the method for assessing the relative security risks posed by different nuclear facilities and transport legs that I was proposing could be implemented in practice. In this example, I used two modestly different implementations of the proposed method to rate the risks of nuclear theft in several countries, ranging from countries with very high threats (such as Russia and Pakistan) to countries with quite low threat levels (such as Japan). One of these implementation approaches focused on directly estimating the probability that a theft attempt that occurred in a particular country would be in each of several bins of capability and the probability that an attempt in any particular bin of capability would be successful in defeating the security measures in place in that country. The other approach focused on giving each country a 1-5 rating on threat level and a 1-5 rating on security level, based on as objective criteria as possible, and estimating how such ratings might translate into probabilities of successful theft. Both approaches used the discount factors developed earlier in the chapter. The results of the two approaches were generally consistent, though not in every detail.

This illustrative assessment made clear that the risks of nuclear theft in Russia and Pakistan remain unacceptably high, given the extremely high threats in these countries, the nuclear weapons and high-quality nuclear materials that exist there, and the improved but still moderate security measures in place. It also made clear, however, civilian research reactors fueled with HEU may pose significant risks even if they are in relatively low-threat countries, if they have significant amounts of relatively high-quality HEU on-site and modest security measures.

In the final section of Chapter 4, I pointed out that in assigning policy priorities, such risk assessments have to be integrated with opportunity assessments, so that easy opportunities for further reducing risk at moderate-risk sites or transport legs will not be missed (and the need for new approaches can be identified early for high-risk sites or transport legs where lack of cooperation seems to suggest little opportunity for progress).

What Policy Tools Are Likely to be Most Effective?

In Chapter 5, I examined the structure and dynamics of the global nuclear security system – how security levels at different facilities and transport legs are determined in an ongoing dynamic between the management of those elements and national regulators, with only limited international influences on the performance of the nuclear security systems in individual countries. There are no specific, binding global standards for nuclear security, though international recommendations, very general international agreements, and international technical cooperation have had a substantial influence on national approaches in many countries.

This examination first outlined the global nuclear security system's structure, with the system elements and feedbacks among them. I then examined the great extent to which changes in the system are driven by responses to particular incidents or investigations. I highlighted the importance of regulation in the overall nuclear security system, as few managers will invest their scarce resources in nuclear security when they are not required to do so. The next sections outlined certain key properties of the system and contraints on improved system performance (as measured by reduced risk of nuclear theft), including:

- Constraints imposed by complacency about the threat and the adequacy of existing measures to address it; structural disincentives (in particular, the circumstance that the costs of preventive action are immediate and visible while the benefits from thefts prevented that might not have occurred anyway are highly uncertain and accrue at some unknown point in the future) and effective policy resistance (the tendency of affected parties to push back against those attempting to impose new policies, such as stricter regulations, that impact their own interests).
- Delays and institutional lock-in, each of which greatly limit the system's ability to respond to changing threats and adapt as quickly as terrorists and other potential adversaries may be able to do. This discussion described cases in which new security rules or new cooperative programs to improve security took years to have their effect – during which time they tend to be weakened, as the compelling urgency felt in the aftermath of a particular incident (such as the 9/11 attacks) tends to decline over time.
- Constraints on what international agreements and cooperation are feasible imposed by the secrecy surrounding nuclear stockpiles and their security arrangements and concerns over national sovereignty. These issues have repeatedly slowed or prevented cooperation and agreements that would otherwise have served all parties' interests.

As illustrations of these constraints, Chapter 5 recounted (a) the history of delays and policy resistance in implementing realistic testing of security system performance in defeating armed outsider attacks at sites regulated by the U.S. NRC and (b) the degree to which, even after the 9/11 attacks, it proved impossible internationally to reach international agreement on the need for stringent nuclear security measures, or to rapidly expand cooperation to improve nuclear security. This assessment of the global nuclear security system's structure and behavior is a tool for structuring thinking about how different proposed policy measures might fare in seeking to improve the system's performance.

The second half of Chapter 5 then turned to a discussion of the record of various policy tools, from negotiation of binding multilateral agreements to bilateral technical cooperation, in seeking to improve security for nuclear stockpiles around the world. For each policy tool, after examining the record, I assigned ratings on a 1-5 scale on each of three criteria: the speed with which the policy tool achieved security improvements; the magnitude of the improvements achieved; and the breadth of applicability of the tool. I then drew tentative lessons learned from the experience with each tool.

This examination led to four overall conclusions:

- Success requires convincing countries that there is a real threat to their own security that needs to be addressed.
- Negotiations by mid-level officials are not likely to overcome the huge systemic obstacles to agreement on in-depth nuclear security cooperation or stringent nuclear security standards. There is some record, however, of accords at top political levels succeeding in sweeping these obstacles aside.
- Partnership-based approaches, demonstrably designed to serve the interests of all parties and incorporating ideas and resources from all parties, tend to have higher success rates (though they may take longer to start up, given the need to build in the ideas of multiple actors).
- Success is likely to require putting in place strong incentives to achieve effective nuclear security – at the levels of states, of key ministries within those states, of facility managers, and of individuals and teams on the staff of particular sites.

All of the policy tools examined showed a significant degree of effectiveness. In particular, purely advisory international recommendations have been more effective than many people might expect, as many countries with relatively little indigenous expertise in these areas have effectively adopted them wholesale (and some suppliers have required them to do so, shifting them from purely advisory to binding requirements). The optimal policy approach to this problem is likely to combine all or nearly all of these tools, with different emphases in different circumstances.

One clear conclusion, however, is that global nuclear security standards sufficient to ensure that nuclear stockpiles are well protected against the threats that terrorists and criminals have shown they can pose are not likely to be achieved through multilateral negotiation of binding treaties or conventions. These talks, carried out at a working level where each countries' representatives tend to be closely tied to the industries and institutions that would have to bear the costs of more stringent standards and where these representatives have little authority to agree to arrangements that would require significant changes in their own countries' practices, have so far resulted in least-common-denominator outcomes that have only a modest effect on security on the ground and take a very long time to achieve that effect. Rather, it seems likely that the best chances for achieving effective global nuclear security standards will be through voluntary political commitments made at a high political level. The challenge is to develop approaches that are specific enough to be effective and that countries can be held accountable for meeting, while being general enough to be accepted by many countries at a high political level.

A second striking result of the examination was the high effectiveness of both on-the-ground technical cooperation and material removals. Material removal, of course, achieves the highest possible level of security, eliminating the risk of theft from a particular site entirely; in some cases, material removal policies have succeeded in doing so relatively rapidly, and the approach is potentially applicable to a large number of nuclear sites around the world. Technical cooperation can never reach quite the same level of security and raises

inevitable issues relating to security culture and sustainability – but large improvements in security have been achieved at a wide range of sites in the former Soviet Union and other countries, sometimes quite rapidly.

Extendable Knowledge

This dissertation has focused very specifically on the issues of nuclear theft and terrorism; it includes a relatively modest quantity of readily extendable knowledge. Perhaps the most important extendable contribution is the approach of explicitly modeling terrorist threats not as a particular point-level of capability as suggested by the design basis threat (DBT) methodology, but as a spectrum with different probabilities of different levels of threat. This conceptual approach is comparable to the transition in safety analyses from focusing on a system's ability to survive a particular design-basis level of earthquake or storm to looking at the system's probability of surviving given the expected frequency of events of different magnitudes. This threat-spectrum approach can and should be applied more broadly to assessing how resources for protecting targets from terrorist attack should be allocated. A paper on conceptual approaches to allocation of protection resources, using this approach among others, is in preparation.

More broadly, the explicitly risk-based approach used here is only occasionally used in assessing security problems, as opposed to safety problems. I would argue that while such probabilistic approaches inevitably require some educated guesses about the chances of different types of threats, more qualitative approaches involve such guesses as well, but in an implicit manner that often leaves room for important misjudgments to go undetected and undebated. This probabilistic approach should be more broadly applied to a wide range of security problems, whether they relate to security against terrorism or against crime. Similarly, the approach used in Chapter 4, making judgments about the probability that particular classes of adversary could accomplish particular goals with particular kinds of nuclear material, could be applied more broadly to analyses of proliferation resistance of nuclear energy systems.

The methodologies used in Chapter 5, including (a) attempting to understand the structure of the elements in a policy system and the feedbacks among them, in order to understand the system's overall behavior; and (b) applying consistent criteria to judge the record of a range of competing or complementary tools for addressing a particular policy problem, are not novel. But they are remarkably rarely used and should probably be used more frequently, to improve the quality of policy choices. In particular, I am not aware of other studies that have used them together, so that an understanding of system structure and behavior can help improve the understanding of the record of different tools in improving the performance of that system.

Areas for Further Research

This dissertation is by no means the final word on the subjects discussed; a broad range of additional research is needed to clarify the risks of nuclear terrorism and how they might best be reduced. The mathematical model presented in Chapter 3 provides a structure for thinking through areas where additional research would be most fruitful, and many of the

most important uncertainties and areas of research that could reduce them are discussed there. In essence, the key questions are: what barriers have been most important in preventing nuclear terrorism to date; how might those barriers (and means and motivations for overcoming them) change in the future; and what policy measures are likely to be most effective in raising or maintaining these barriers, reducing the risk of nuclear terrorism in the future?

In particular, more research is needed to clarify:

- Which terrorist groups are currently interested in nuclear terrorism; what relevant capabilities they have or may be putting together; what level of organizational effort they are devoting to nuclear projects; what factors have so far prevented these efforts from progressing further; what factors have so far limited the level of organizational effort these groups have devoted to nuclear matters and led other terrorist groups not to pursue nuclear terrorism seriously; and how might these factors change in the future;
- What role organized terrorist groups or organized criminal groups have so far played in nuclear theft and smuggling, and what factors might cause this past experience to be different in the future;
- The quantity and quality of nuclear weapons and weapons-usable material at all relevant sites around the world (including, for example, the amounts of both fresh and irradiated highly enriched uranium (HEU) at research reactors throughout the world) and the types and frequency of transports of these items that occur in different countries;
- Plausible insider and outsider threats in different countries – including the types of capabilities that terrorists and criminals have brought to bear in attacks or thefts from guarded facilities in each country; morale, pay, corruption, ideology, and crime among the staff and guards at nuclear facilities and transport legs; and related factors;
- The specific security measures in place for different nuclear facilities and transport legs, and how effective they would likely be in defeating different types of insider and outsider capabilities that might be brought to bear in a theft attempt (taking into account both equipment in place and personnel performance);
- Processes for making decisions on nuclear security measures and resources for them in different countries and approaches to influencing those decisions (including the attitudes of key players toward the threat and toward specific means for reducing it);
- The range of different policy options available for achieving increases in security for nuclear stockpiles in different countries and which, in which combinations, are likely to be most effective, under which particular circumstances;
- The chances that states might consciously decide to provide nuclear weapons or the materials to make them to terrorist groups; what factors affect these probabilities and how those factors might change in the future; what policy steps could reduce the probability that a state such as North Korea would decide to transfer nuclear weapons or materials to

others and the probability that they would succeed in doing so, and what magnitude of reduction in these probabilities might plausibly be achieved; and

- What other policy measures, in addition to improved nuclear security, could be most effective in reducing the risk of nuclear terrorism (from strengthened counterterrorism efforts focused on plausible nuclear terrorist groups to beefed-up efforts to interdict nuclear smuggling).

In particular, there are two issues that are essential to the success of efforts to achieve effective security for nuclear stockpiles for the long haul, which I have only briefly discussed in this dissertation: security culture and sustainability. A great deal of additional research is needed to understand the most effective approaches to achieving these objectives.

Security Culture

Security culture – the habit, among all security-relevant personnel, of taking security seriously and taking the actions needed to ensure high security – is a critical element of nuclear security. If security doors are left propped open for convenience, guards patrol without ammunition in their guns to avoid accidental firing incidents, and security personnel turn off alarm systems out of annoyance with their false alarms,[1] good security is not likely to be achieved.[2] As Gen. Eugene Habiger, former DOE "security czar" and former commander of U.S. strategic forces, put it: "good security is 20% equipment and 80% culture."[3]

Unfortunately, changing any deeply ingrained aspect of organizational culture, including security culture, is very difficult to do.[4] In general, these changes do not occur

---

[1] All of these are behaviors that have been observed at sites in Russia where U.S.-funded Material Protection, Control, and Accounting (MPC&A) cooperation is taking place. All of these are also behaviors that have been observed at U.S. sites in the past.

[2] Approaches that provide "inherent security" with limited reliance on human intervention – putting nuclear material in a steel cage that would take a long time to cut through, piling huge concrete blocks in front of the door, and the like – are a partial exception. Such technologies, however, are typically only applicable to items that are in long-term storage, not in regular use. Moreover, staff with little regard for security can undermine even these approaches' effectiveness – by not replacing the concrete blocks after the room has been accessed, for example, to make it more convenient to get in again the next day or the next week. And even these approaches offer only delay, ultimately relying on human intervention to stop adversaries from getting at the weapons or materials being protected.

[3] Interview by author, April 2003.

[4] A classic text on organizational culture (though one much critiqued in some circles) is Edgar H. Schein, *Organizational Culture and Leadership*, Third ed. (San Francisco, CA: Jossey-Bass, 2004). For a shorter and less theoretical account from the same author, see Edgar H. Schein, *The Corporate Culture Survival Guide* (San Francisco, CA: Jossey-Bass, 1999). For an assessment of different approaches to analyzing organizational culture that critiques the "functionalist" approach of these volumes (that is, an approach that focuses on analyzing which elements of a culture supposedly contribute to or detract from a particular function and then on changing those elements so that the organization performs that function better), see Joanne Martin, *Organizational Culture: Mapping the Terrain*, First ed. (Thousand Oaks, CA: SAGE Publications, 2002). There are countless corporate how-to books on corporate cultures and how to change them to improve an organization's ability to meet a particular goal (some of which include quite a number of cases of failure of such culture-change efforts). See, for example, John P. Kotter, *Leading Change*, First ed. (Boston, MA: Harvard Business School Press, 1996). Some of these how-to books are focused on how to change an organization's

unless the top leaders of the organization dedicate themselves to making them happen and devote a substantial and sustained effort to the task[5] – which means that the first job is to convince senior nuclear managers of the importance of achieving strong security cultures in their organizations. As the string of security incidents at the Los Alamos National Laboratory in recent years makes clear, the United States still faces major challenges with security culture even at facilities where the U.S. government sets all the rules and provides all the funding.[6] Trying to improve security culture in other countries, whose national cultures U.S. officials may not understand well and where U.S. programs have their hands on few of the levers of power, poses a far greater challenge – but a crucial one. Assessing how well programs are doing in meeting this challenge is also extraordinarily difficult, requiring the development and use of a variety of partial and indirect indicators of progress.

Of course, organizations have been attempting to select, train, and motivate people to provide high levels of security for valuable goods for centuries. But the literature actually analyzing how to achieve strong security cultures is surpringly thin. Government efforts to improve nuclear security culture that are now underway are largely learning by doing while drawing heavily on analogies from the decades-long effort to improve *safety* cultures, in the nuclear industry and elsewhere. The IAEA, for example, has issued dozens of publications over almost twenty years on safety culture and has an extensive and successful program in promoting safety culture, but has yet to complete its first publication specifically on security culture (though one is in development).[7] U.S. and Russian officials have agreed to work to promote security culture and have launched a program for doing so, but often run into debates concerning not only what specific steps should be taken but even what issues are or are not part of the concept of "security culture." Only recently have in-depth examinations of the

---

safety culture: see, for example, Terry E. McSween, *The Values-Based Safety Process: Improving Your Safety Culture with Behavior-Based Safety* (Hoboken, N.J.: Wiley-Interscience, 2003).

[5] See, for example, discussion in Kotter, *Leading Change*.

[6] For statements attributing the ongoing problem at Los Alamos to the security culture at the laboratory, see, for example, House Committee on Energy and Commerce, Energy and Air Quality Subcommittee, *A Hearing to Review Proposals to Consolidate the Offices of Counter Intelligence at NNSA and DOE*, 13 July 2004 (available at http://energycommerce.house.gov/108/Hearings/07132004hearing1346/hearing.htm as of 15 August 2005). For a remarkable official excoriation of the security culture at the Department of Energy and its predecessors, stretching back over decades, see President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington D.C.: PFIAB, 1999; available at http://www.fas.org/sgp/library/pfiab/ as of 13 December 2006). This report lays blame for much of the security problem at DOE on cultural attitudes toward security, which it describes in stark terms: "Never have the members of the Special Investigative Panel witnessed a bureaucratic culture so thoroughly saturated with cynicism and disregard for authority.... DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility to security issues... The predominant attitude toward security and counterintelligence among many DOE and lab managers has ranged from half–hearted, grudging accommodation to smug disregard."

[7] A workshop on security culture has been developed and offered on a couple of occasions, but is still considered developmental; a publication with guidance on improving security culture is still in preparation. Interviews with officials from the IAEA Office of Nuclear Security, November 2004, October 2005, and July 2006.

problem of security culture begun to appear – but even these recent treatments do not present detailed, actionable recommendations for improving nuclear security cultures.[8]

There is an urgent need for further research to better understand what approaches to strengthening security culture are likely to be most effective and how these might vary from one national and organizational context to the next. Remarkably little work has been reported in the open literature to date that focuses on soliciting the views of people who currently manage high-security organizations – whether nuclear facilities that have a reputation for particularly strong security culture, or other facilities where high levels of security are required.

In particular, in the nuclear world, most managers take primarily the security measures the government requires them to and have little direct incentive to think creatively about how security performance might be improved. For some private sector facilities, however, security (especially against insider theft) is crucial to the bottom line, and managers of these facilities have for many years had direct profit incentives to find ways to strengthen security culture among their employees. Case studies and interviews with managers of casinos (where large amounts of money are constantly changing hands, and the profit margin may be a few percent), gold processing facilities (analogous in some ways to HEU or plutonium processing facilities), and plants that legally manufacture narcotics and other drugs that command high prices on the black market (also analogous to HEU or plutonium processing facilities) could provide substantial new insights into measures to develop and improve security culture, especially if coupled with similar case studies and interviews with managers of nuclear facilities and high-security military facilities. There is also much more to be done in exploring the analogy with safety culture (and that analogy's limits), focusing particularly on learning lessons from the comparison of successful and failed efforts to improve safety culture in different organizations.

Sustainability

If the United States and other nations spend billions of dollars installing improved equipment for securing and accounting for nuclear stockpiles around the world, and that equipment is broken and unused five years later, the objective of ensuring that these stockpiles are not stolen will not be achieved. Hence it is critical that efforts to upgrade nuclear security be designed not only to get the job done quickly, but also to include putting in place an overall system of resources, incentives, and organizations that will ensure that effective security for these stockpiles is maintained for the long haul, long after international assistance comes to an end. The watchword used for this objective in the U.S.-funded programs to improve nuclear security is "sustainability."[9]

---

[8] The best of these recent accounts is Igor Khripunov and James Holmes, eds., *Nuclear Security Culture: The Case of Russia* (Athens, Georgia: Center for International Trade and Security, The University of Georgia, 2004; available at http://www.uga.edu/cits/documents/pdf/Security%20Culture%20Report%2020041118.pdf as of 18 February 2005).

[9] A committee of the National Research Council has suggested using the term "indigenization" instead, arguing that "sustainability" implies sustaining exactly the approaches put in place with international assistance, rather than adapting those approaches to local circumstances over time. See Committee on Indigenization of Programs

Here, too, U.S., Russian, and other officials are working diligently to put in place measures to ensure that improved nuclear security will be sustained after international assistance phases out. But with very little research on the determinants of sustainability in this context, they are, in effect, learning by doing.

Sustainability can be broken into two parts: the *ability* to provide effective nuclear security for the long haul and the *motivation* to apply the necessary resources to do so. Most sustainability efforts to date have focused on ability – establishing training programs so that there will be adequate trained personnel to operate and maintain effective nuclear security systems, creating maintenance and spare parts infrastructures so that equipment can be fixed and replaced, and contracting with sites to lay out plans for operating and maintaining their new security systems and estimate the money and manpower needed to implement them.

But motivation, or commitment, will be equally important: the United States and other donor countries are making investments in improving nuclear security in foreign countries largely because those foreign countries do not assign as high a priority to nuclear security as the donors think they should. Russia, in particular, with a sophisticated nuclear infrastructure, a growing economy, and a federal budget in surplus, would certainly be able to provide effective security for its nuclear assets without U.S. help, *if* it made nuclear security a real priority. But today, while major improvements have been made, Russia continues to underinvest in nuclear security and to allow ineffectual regulation, corrupt and ineffective guard forces, and other serious weaknesses to continue, as discussed in Chapter 2. Unless Russia and other recipient states increase the priority they assign to nuclear security, much of the progress made with international assistance may evaporate within a few years after international assistance phases out.

A critical question, then, is how to change a foreign government's assessment of the level of priority it should devote to nuclear security. This, of course, is only one specific case of a type of problem that arises frequently: what to do about cases where the allocations of priorities or governance weaknesses in one country affect the well-being of other countries? How can one country that thinks an issue is a high priority convince another country where the issue is unfolding to take it seriously? Among the countless examples of this class of problems are control of pollution in one country that affects the countries downwind or down-river; effectiveness of efforts to prevent terrorist or organized crime groups from using countries as bases of operations; control of illegal flows of drugs, money, and other contraband; enforcement of export controls; and control of pirating of intellectual property. We are moving into an age in which the quality of governance in every country is the legitimate concern of all countries.

---

to Prevent Leakage of Plutonium and Highly Enriched Uranium from Russian Facilities, Office for Central Europe and Eurasia, National Research Council, *Strengthening Long-Term Nuclear Security: Protecting Weapon-Usable Material in Russia* (Washington, D.C.: National Academy Press, 2005; available at http://fermat.nap.edu/catalog/11377.html as of 4 April 2006). While this suggestion has some merit, I have stayed with the term "sustainability" here because it is much more broadly used among program participants, and I do not believe that it strongly implies keeping nuclear security and accounting systems and approaches exactly as they were.

Yet remarkably little research seems to have been done on the questions of how governments can seek to make long-term changes in other governments' assignment of priorities to particular issues, or how a government's performance in particular government functions can be improved in a way that will last long after the capacity-building assistance has come to an end. The limited available literature suggests that improvements in such activities are much more likely to be long-lasting when:

- The improved capacity provides very direct benefits to the participants that make it profitable for them to invest their time and resources in continuing it after international assistance comes to an end (and they have the capacity to do so). This might be the case, for example, for projects that provide participants the resources to start sustainable and profitable businesses.[10] This is not likely to be the case for nuclear security programs, which cost money without generating revenue. There are a variety of options, however, for providing incentives for strong security performance at the levels of individuals and teams, facilities, and states, which could contribute significantly both to building strong security cultures and to the prospects for sustainability.[11]
- Recipient governments are motivated to improve performance in the area in question, and international assistance focuses not only on providing technical equipment and training, but on the entire governmental system for performing the function at issue, including the power, resources, and effectiveness of the agencies responsible for the function, the effectiveness of decision-making processes, and processes for recruiting, training, and retaining appropriate personnel.[12]
- International assistance takes a partnership-based approach, in which recipients are intimately involved in deciding what should be done and why – and in that process, become convinced of the need for the new approaches.[13]

But these lessons are tentative and are not yet based on any in-depth comparisons of successful and failed cases of attempts to make long-lasting improvements in the commitment

---

[10] For a useful discussion of one such case and its implications, see Martin Fisher, "Income Is Development: Kickstart's Pumps Help Kenyan Farmers Transition to a Cash Economy," *Innovations* 1, no. 1 (Winter 2006; available at http://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2006.1.1.9 as of 29 December 2006).

[11] Matthew Bunn, "Incentives for Nuclear Security," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

[12] See Merilee S. Grindle, ed., *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries* (Cambridge, Mass.: Harvard University Press, 1997).

[13] For a detailed argument along these lines, see Albert R. Wight, "Participation, Ownership, and Sustainable Development," in *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries*, ed. Merilee S. Grindle (Cambridge, Mass.: Harvard University Press, 1997). For arguments for the benefits of such partnership-based approaches with respect to nuclear security, see U.S. and Russian Committees on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, U.S. National Academy of Sciences and Russian Academy of Sciences, *Strengthening U.S.-Russian Cooperation on Nuclear Nonproliferation: Recommendations for Action* (Washington, D.C.: National Academy Press, 2005; available at http://books.nap.edu/catalog/11302.html as of 15 November 2005); Matthew Bunn, "Building a Genuine U.S.-Russian Partnership for Nuclear Security," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Phoenix, Ariz.: INMM, 2005; available at http://bcsia.ksg.harvard.edu/BCSIA_content_stage/documents/inmmpartnership205.pdf as of 2 January 2007).

and performance of foreign governments in particular areas. Promising areas for further research include: (a) case studies and interviews with managers and staff at key nuclear facilities that appear to have either high motivation and capacity to sustain high levels of nuclear security, or low motivation and capacity, to seek to tease out the causes of such differences; (b) focused comparison case studies of past capacity-building assistance programs, to try to learn lessons concerning what factors most affect the probability that increases in government performance achieved through such programs will last;[14] (c) focused comparison case studies of past cases of attempts to convince countries to take actions to which they initially assigned low priority (from rain forest preservation in Brazil to intellectual property protection in China), to attempt to learn lessons concerning which approaches seem to work more often than others; (d) focused comparison case studies of attempts to build international norms of high performance in particular sectors (ranging from airline safety to financial controls), looking for lessons on what factors most influence the chance of success.

In the case of nuclear security in particular, it seems clear that both security culture and sustainability depend fundamentally on a belief that the threat is real and urgent. Unless the key officials of each government with nuclear weapons or weapons-usable materials believe that nuclear terrorism is a real threat to *their* country's security, not simply something the Americans are worried about, they are unlikely to take the steps needed to build a strong security culture and a lasting nuclear security system. Hence, policy measures focused on getting key officials and managers to grasp the reality of the threat may be among the most important steps that need to be taken – as discussed in the recommendations below.

Policy Recommendations

The United States and other leading governments should launch a fast-paced global effort to reduce the risk of nuclear terrorism.[15] As a first step, this effort should focus on ensuring that every nuclear warhead and every significant stock of weapons-usable material worldwide is secured and accounted for to standards adequate to defeat the threats that terrorists and criminals have shown they can pose in the country where that stock exists. Success will require a sea-change in the level of sustained leadership from the highest levels of the governments involved, focused on overcoming obstacles to and identifying opportunities for rapid progress.

Improving Nuclear Security

The United States and other leading governments should put improving security for nuclear warheads and materials high on the diplomatic agenda – an issue to be addressed with every country with stockpiles to secure or resources to help, at every level, at every

---

[14] An initial step in this direction is offered by Grindle, ed., *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries*. But that book and the subsequent literature does not really attempt to examine capacity-building programs 5-15 years after they have come to an end, to see which ones in fact had a lasting effect and which did not.

[15] These recommendations draw heavily on those in Matthew Bunn and Anthony Wier, *Securing the Bomb 2006* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2006; available at http://www.nti.org/securingthebomb as of 23 July 2006), pp. 121-157.

opportunity, until the job is done. The effort should be driven by a genuinely prioritized plan, adapted as the effort proceeds, focusing on those sites and transport legs where there are the largest opportunities for reductions in risk (as described in Chapter 4). Each of the policy tools described below, from a global coalition to forge new political-level commitments to nuclear security, to bilateral cooperation on security upgrades, to negotiation of more effective global standards for nuclear security, should be used in an integrated way to achieve the overall objective of ensuring that every nuclear warhead and every stock of HEU and plutonium worldwide is secure enough so that the risk of nuclear theft and terrorism it poses is very low – rather than each of these tools being pursued independently, often by officials with little awareness of what efforts on other tracks are doing and the potential implications, as is currently the case. That effort will not only require flexible use of several policy tools, but several key changes in approach as well, which are also described below.

There is still much to be done in Russia, to complete the cooperative upgrades now under way, ensure that security measures are put in place that are sufficient to meet the threats that exist in today's Russia, forge a strong security culture, and ensure that high levels of security for nuclear stockpiles will be sustained after international assistance phases out. But increasingly, the work with Russia should become a true partnership of near-equals, framed as one part of a global approach – and the United States should redouble its efforts to expand its programs to prevent nuclear terrorism across the globe.[16] The recommendations below, therefore, while applicable to the work in Russia, are global in nature.

A Global Coalition to Prevent Nuclear Terrorism

A number of authors, including this one, have long advocated the formation of a global coalition of countries focused on pursuing their shared interest in reducing the risk of nuclear terrorism.[17] Such a coalition could provide a mechanism for gaining high-level political commitment to taking the needed steps to reduce nuclear terrorism risks, potentially overcoming the obstacles that tend to arise at the working level, as described in Chapter 5.

---

[16] For an especially useful discussion of specific approaches to strengthening U.S.-Russian nuclear security cooperation through partnership-based approaches, written jointly by U.S. and Russian experts, see U.S Committee on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, National Research Council, and Russian Committee on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, Russian Academy of Sciences, *Strengthening U.S.-Russian Cooperation on Nuclear Nonproliferation* (Washington, D.C.: National Academy Press, 2005; available at http://fermat.nap.edu/catalog/11302.html as of 2 January 2007). See also Bunn, "Building a Genuine U.S.-Russian Partnership for Nuclear Security."

[17] See, for example, Richard Lugar and Sam Nunn, "Connecting the Dots on Nuclear, Biological, and Chemical Terrorism: The Clear Danger and the Imperative of a Global Coalition Response" (Washington, D.C.: Nuclear Threat Initiative, 27 May 2002; available at http://www.nti.org/c_press/statement_nunnlugar_052702.pdf as of 22 December 2006); Graham T. Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004); Bunn and Wier, *Securing the Bomb 2006*. A somewhat similar suggestion to create a "Contact Group to Prevent Nuclear Terrorism," including many of the G8 states along with China, India, Pakistan, Israel, and other states with weapons-usable nuclear material that wish to join, is outlined in George Perkovich et al., *Universal Compliance: A Strategy for Nuclear Security* (Washington, D.C.: Carnegie Endowment for International Peace, 2005; available at http://www.carnegieendowment.org/files/UC2.FINAL3.pdf as of 21 March 2005), pp. 87-88.

In July 2006, President Bush and President Putin announced the launch of the Global Initiative to Combat Nuclear Terrorism.[18] At the initiative's founding meeting, in Rabat, Morocco, in October 2006, the initial participants agreed on a very general statement of principles.[19] These statements included few specifics, however: now is the time to put the meat on these bones and to build the Global Initiative into the fast-paced global effort to reduce the risk of nuclear terrorism that is urgently needed. President Bush should immediately begin working with the founding Global Initiative members and other key states with nuclear weapons or weapons-usable nuclear materials to gain agreement that the participants in this initiative will:

- Ensure that all stockpiles of nuclear weapons and weapons-usable materials under their control would be protected at least to a common security standard, sufficient to defeat the threats terrorists and criminals have demonstrated they can pose. (Participants would be free to protect their stockpiles to higher standards if they perceived a higher threat in their country.) For example, the commitment could be to provide protection at least against two small groups of well-armed and well-trained outsiders, one to two well-placed insiders, or both outsiders and insiders working together.
- Work with other states to convince them to join the commitment to this common standard and provide assistance where necessary to help countries put this level of security in place.
- Develop and put in place transparency measures that will help build international confidence that the agreed security measures have in fact been taken, without providing public information that would be helpful to terrorists.
- Sustain security levels meeting the agreed standard indefinitely, using their own resources, after any international assistance they may be receiving comes to an end.
- Reduce the number of locations where nuclear weapons and weapons-usable nuclear materials are located, achieving higher security at lower cost.
- Put in place border and transshipment controls that would be as effective as practicable in interdicting nuclear smuggling, as required by United Nations Security Council Resolution (UNSCR) 1540, and help other states around the world to do likewise.
- Drastically expand intelligence and law enforcement sharing related to indicators of nuclear theft risks, nuclear smuggling and criminal networks that might contribute to those risks, groups with ambitions to commit catastrophic terrorism, and other subjects related to preventing nuclear terrorism.

---

[18] "Joint Statement by U.S. President George Bush and Russian Federation President V.V. Putin Announcing the Global Initiative to Combat Nuclear Terrorism" (St. Petersburg, Russia: The White House, Office of the Press Secretary, 15 July 2006; available at http://www.whitehouse.gov/news/releases/2006/07/20060715-2.html as of 22 December 2006).

[19] "Statement of Principles by Participants in the Global Initiative to Combat Nuclear Terrorism" (Washington, D.C.: The White House, Office of the Press Secretary, 31 October 2006; available at http://www.state.gov/r/pa/prs/ps/2006/75405.htm as of 22 December 2006).

- Pass laws making actual or attempted theft of a nuclear weapon or weapons-usable nuclear material, unauthorized transfers of such items, or actual or attempted nuclear terrorism crimes comparable to treason or murder.
- Cooperate to strengthen nuclear emergency response capabilities – including nuclear materials search capabilities that could be deployed rapidly anywhere in the world in response to an unfolding crisis.
- Exchange best practices in security and accounting for nuclear warheads and materials – to the extent practicable – as is already done in the case of nuclear safety.
- Strengthen the ability of the IAEA to contribute to preventing nuclear terrorism.
- Take such other actions as the parties agree are needed to reduce the risk of nuclear terrorism.

This global coalition should include the Group of Eight (G8) industrialized democracies, along with China, India, Pakistan, and, ideally, Israel (which is believed to have a significant stockpile of nuclear weapons) and South Africa (which once had nuclear weapons and still has one of the largest stockpiles of highly enriched uranium (HEU) among the developing non-nuclear-weapon states). Offering these states roles as co-leaders, with the world's leading nuclear states, of a global effort to improve all participants' security will be much more politically appealing than framing cooperation as a matter of assistance necessitated because they were unable to properly secure their own stockpiles. Between them, these countries have all of the world's nuclear weapons (except for the handful that may exist in North Korea) and more than 95% of the world's weapons-usable nuclear material. If they were all participating, it is likely that other states with smaller amounts of HEU or separated plutonium would sign up as well.

To be effective in accelerating and strengthening global efforts to reduce the risk of nuclear terrorism, the coalition would need a strong mechanism for ensuring that the initial commitments were followed through. The participants should each designate senior officials to be responsible for all aspects of implementing the global coalition commitments, and these senior officials should meet regularly to develop agreed plans with measurable milestones, to oversee progress in implementation, and to develop means to overcome obstacles. In particular, the coalition partners should agree on a target of putting in place security measures sufficient to meet the agreed minimum standard for all stockpiles of nuclear weapons and weapons-usable materials worldwide within six years or less. Since this would be an operational initiative going well beyond the G8, this group should be a standing organization. It should report to the leaders of the participating states on a regular basis, perhaps once every six months. Such a mechanism would help to avoid the fate of past summit initiatives, which have sometimes been announced with great fanfare and then went nowhere when the summit spotlight was gone.

This coalition would be focused on taking concrete actions to reduce the risk of nuclear terrorism – and in particular, on ensuring that every nuclear weapon and every kilogram of nuclear material worldwide is secure and accounted for. The goal would be to

accomplish that objective as quickly and effectively as possible. In many cases, this would mean countries taking action to improve security for their own stockpiles, perhaps with a modest amount of international advice and exchange of best practices. In others, U.S. or other international funding or expertise might be critical to getting the job done effectively and quickly.

Those participating states in a position to help fund the efforts of others should collectively make substantial pledges of funds for implementing the needed actions around the world. These efforts could draw on funds pledged for an earlier initiative, the Global Partnership Against the Spread of Weapons and Materials of Mass Destruction announced at the G8 summit in Kananaskis, Canada, in 2002.[20] To date, unfortunately, the Global Partnership has nothing global about it except its name, and only a dribble of non-U.S. funds in the Global Partnership has so far been focused on improving nuclear security measures. Instead, the Global Partnership is almost entirely focused within Russia (now with Ukraine as an added recipient), and the non-U.S. funds have primarily been devoted to chemical weapons destruction and submarine dismantlement (the two areas Russia's requests have focused on most intensely). While the participants in the Global Partnership initially pledged $20 billion to the effort over 10 years, pledges from specific countries remain more than $2 billion short of that target and appear to have leveled off.

It may be that a new mission, to contribute to preventing nuclear terrorism throughout the world – and to implementing the other steps to control weapons and materials of mass destruction mandated by UNSCR 1540 (discussed in more detail below) – could convince some states to provide additional contributions, bringing the total up to the $20 billion initial target or more and providing sufficient funds to implement the needed steps for all countries requiring assistance worldwide.[21] (The number and magnitude of the upgrades needed around the world are not publicly known, making it difficult to reliably estimate the total cost of the needed upgrades, but it seems likely that a total substantially less than the $20 billion originally pledged to the Global Partnership would be sufficient to drastically reduce the global danger of nuclear theft and terrorism.) This mission would return the Global Partnership to its original ambitions, which included a commitment to take the steps necessary to "prevent terrorists, or those that harbor them, from acquiring" the materials needed for weapons of mass destruction; specifically called on "all countries," not just Russia, to join in providing effective security and accounting for their stockpiles of nuclear weapons and weapons-usable nuclear materials; and offered assistance to any country needing help to provide such effective security.[22] The coalition participants should commit to providing the

---

[20] "The G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction" (Kananaskis, Canada: Government of Canada, 27 June 2002; available at http://www.g7.utoronto.ca/summit/2002kananaskis/arms.html as of 27 June 2006). For a useful summary of the Global Partnership as of mid-2006, with recommendations for next steps, see *Assessing the G8 Global Partnership: From Kananaskis to St. Petersburg* (Washington, D.C.: Strengthening the Global Partnership Project, Center for Strategic and International Studies, 2006; available at http://www.sgpproject.org/publications/SGPAssessment2006.pdf as of 22 December 2006).

[21] I am grateful to Robert Einhorn for this suggestion. Personal communication, December 2006.

[22] "The G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction".

resources necessary to ensure that lack of funding does not constrain the pace at which nuclear stockpiles around the world can be secured and consolidated. As the senior contact group develops more detailed plans, they should be tasked with estimating the costs of implementation, and coalition members should make pledges sufficient to implement them at the fastest practicable pace.

The coalition partners should act to give states and facilities strong incentives to provide effective security for their nuclear stockpiles.[23] The United States should work with all states with nuclear stockpiles to ensure that effective and well-enforced nuclear security rules are put in place, giving all facilities with nuclear stockpiles strong incentives to ensure they are effectively secured – including the possibility of being fined or temporarily shut down if a facility does not follow the rules. It would also be desirable to work to convince these states to structure financial and other rewards for strong nuclear security performance (comparable, for example, to the bonus payments contractors managing DOE facilities can earn for high performance). The United States should also establish a preference in all U.S. contracts going to foreign facilities with nuclear weapons or weapons-usable nuclear material (not just those supporting DOE nonproliferation programs) for facilities that have positively demonstrated effective security performance in realistic tests and should seek to convince other leading nuclear states to do the same. Ultimately, effective nuclear security should become a fundamental "price of admission" for doing business in the international nuclear market.

Bilateral Cooperation to Upgrade Nuclear Security

Bilateral cooperation with Russia and with other countries to upgrade nuclear security measures should remain a key policy tool, coming under the rubric of this global coalition. U.S.-Russian cooperation is particularly important. As President Bush and President Putin acknowledged in their Bratislava statement, as the countries with by far the world's largest nuclear stockpiles, the United States and Russia bear a special responsibility for action. They should seek to take such effective action in securing their own stockpiles that they set a strong example for the rest of the global coalition participants. In addition, they should apply their experience to work together to help other countries around the world to secure their stockpiles.

U.S.-Russian bilateral cooperation on improving nuclear security is coming to a climax, as the two sides have agreed on a joint goal of completing security upgrades at an agreed list of nuclear warhead and material sites by the end of 2008. Even if that goal is met, however, a great deal of work to build effective security cultures, ensure sustainability, address the sites not yet covered by joint cooperation, ensure that security measures are sufficient to defeat the large outsider and insider threats that exist in Russia, and embed all these new measures in effective and effectively enforced nuclear security rules will remain to be done. DOE envisions a period lasting from 2008-2013 during which U.S. funding will

[23] Bunn, "Incentives for Nuclear Security."

phase down and Russian funding will phase in, followed by continuing low-level cooperation to exchange best practices and resolve ongoing issues either side may face.[24]

The two countries need to move quickly to agree on their approaches to cooperation in 2008 and beyond. In particular, it is very important for the United States to seek a presidential-level Russian commitment to provide the resources needed to sustain high levels of nuclear security in Russia after international assistance phases out – and to ensure that mechanisms are in place to follow up on implementation of that commitment. Since most nuclear managers will not implement security measures they are not required to put in place, effective regulation will be absolutely central to achieving high levels of nuclear security that last for the long haul, and ongoing cooperation with Russia and with other countries must focus intensely on steps to put effective nuclear security regulation in place. It is also important to work to forge strong security cultures. (See discussion of these points below.)

Whether in Russia or in other countries, the goal of cooperation to upgrade nuclear security should not be only to meet a least-common-denominator standard such as the existing IAEA physical protection recommendations, but to achieve a level of security that reduces the risks of nuclear theft to a low level, given the threats that exist in the country in question and the quantity and quality of the nuclear material at the facilities there. In many cases, this may require more substantial upgrades – or more efforts to convince recipient states to provide more numerous and effective guards – than have yet been undertaken.

Adapting the threat-reduction approaches developed in cooperation with Russia and other former Soviet states to the specific circumstances of each other country where cooperation must go forward is likely to be an enormous challenge. Attempts to simply copy the approach now being used in Russia are almost certain to fail.[25] Cooperation with states with small nuclear weapons arsenals, such as Pakistan, India, China, and Israel, is likely to be especially difficult. For all of these states, nuclear activities take place under a blanket of almost total secrecy, and direct access to many nuclear sites by U.S. personnel is likely to be impossible in the near term (an issue discussed in more detail below). In general, working out arrangements to improve nuclear security – and to build confidence that effective nuclear security really is in place – will require considerable creativity and persistence. Providing security equipment and training in such cases in no way contravenes the United States'

---

[24] U.S. Department of Energy, *2006 Strategic Plan: Office of International Material Protection and Cooperation, National Nuclear Security Administration* (Washington, D.C.: DOE, 2006).

[25] For discussion, see "Challenges of Adapting Threat Reduction to New Contexts," in Matthew Bunn and Anthony Wier, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007), pp. 104-105. See also James E. Goodby et al., *Cooperative Threat Reduction for a New Era* (Washington, D.C.: Center for Technology and National Security Policy, National Defense University, 2004; available at http://www.ndu.edu/ctnsp/CTR%20for%20a%20New%20Era.pdf as of 21 March 2005); Lee Feinstein et al., *A New Equation: U.S. Policy toward India and Pakistan after September 11* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.ceip.org/files/pdf/wp27.pdf as of 4 October 2006); Rose Gottemoeller and Rebecca Longsworth, *Enhancing Nuclear Security in the Counter-Terrorism Struggle: India and Pakistan as a New Region for Cooperation* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.ceip.org/files/pdf/wp29.pdf as of 21 March 2005).

obligation under the Nonproliferation Treaty (NPT) not to assist non-nuclear-weapon states in acquiring nuclear weapons and can be done in a way that is consistent with all U.S. export control laws as well.

Effective Global Nuclear Security Standards

Facing terrorists with global reach, nuclear security is only as good as its weakest link: insecure nuclear material anywhere is a threat to everyone, everywhere. Hence, effective and truly global standards for nuclear security are urgently needed. Because there is a global threat applicable to even the most secure countries, but much higher threats in some countries where terrorists and thieves are especially active and capable, there should be a minimum level of security for all stocks of nuclear weapons and weapons-usable nuclear materials worldwide and more stringent security measures, going beyond the global minimum, where those measures are needed. Recent agreements such as the nuclear terrorism convention[26] and the amendment to the physical protection convention[27] are useful, but provide no specific standards for how secure nuclear weapons or weapons-usable materials should be (nor language from which such standards could be built by agreed interpretation.) The U.S. government and other leading governments should use a variety of policy tools to try to forge effective global nuclear security standards.

Gaining political-level commitments. As discussed in Chapter 5, efforts to negotiate an effective global nuclear security standard in a treaty have not succeeded in the past and are not likely to succeed in the near-term future, as such negotiations inevitably become bogged down by country representatives who see little urgency for action and considerable potential for added costs and unwanted intrusion for the organizations they represent. The most plausible means to overcome such obstacles is for high-level leaders who see the need for a minimum global nuclear security standard, in the interests of all, to quickly put in place a broad political commitment to such a standard. The United States should immediately begin discussions with other leading governments, as part of the effort to forge a global coalition to prevent nuclear terrorism, on a common minimum standard for nuclear security, strong enough to be effective and to make it possible to hold countries accountable for whether they were fulfilling the commitment, but general enough to allow each state to follow the approaches it has found best achieve the security objective in its own context. In some countries, an approach focused on large numbers of armed guards may work best; in others, a technology-heavy approach may be more appropriate. Performance in defeating plausible threats is what is important, not the specific means by which that performance is achieved. Hence, a commitment that nuclear stockpiles will be protected at least against a common

---

[26] *International Convention for the Suppression of Acts of Nuclear Terrorism* (New York: United Nations, 2005; available at http://www.un.int/usa/a-59-766.pdf as of 16 September 2005). This treaty's most specific provision related to security of nuclear stockpiles is a requirement that all parties "make every effort to provide appropriate measures to ensure the protection" of nuclear and radiological materials (Article 8).

[27] *Amendment to the Convention on the Physical Protection of Nuclear Material* (Vienna: International Atomic Energy Agency, 2005; available at http://www-pub.iaea.org/MTCD/Meetings/ccpnmdocs/cppnm_proposal.pdf as of 16 September 2005).

minimum design-basis threat is likely to be the most effective option for the structure of such a standard.

Using UNSCR 1540. One promising approach to following through on such a high-level political commitment is by fleshing out the specifics of what is required by UNSCR 1540. UNSCR 1540, passed unanimously in April 2004, created a new binding legal obligation on every state to provide "appropriate effective" security and accounting for whatever nuclear stockpiles it may have (along with a wide range of other legal obligations to improve controls over weapons of mass destruction and related materials).[28] Unfortunately, little use of this remarkable tool has yet been made – no government or international organization has yet sought to lay out what an "appropriate effective" nuclear security and accounting system includes and to pressure (and help) states to put those legally required measures in place.

This should change. UNSCR 1540 creates an opportunity for the United States to work with other countries and the IAEA to: detail the essential elements of an "appropriate effective" system for nuclear security; assess what improvements countries around the world need to make to put these essential elements in place; and assist countries around the world in taking the needed actions. If broad agreement could be reached on the essential elements of an "appropriate effective" nuclear security system, that would, in effect become a legally binding global standard for nuclear security.[29] Indeed, the entire global effort to put in place stringent nuclear security measures for all the world's stockpiles of nuclear weapons and weapons-usable nuclear materials can be considered simply as the implementation of the unanimously approved obligations of UNSCR 1540.

If the words "appropriate effective" mean anything, they should mean that nuclear security systems could effectively defeat threats that terrorists and criminals have shown they can pose. Thus one possible definition would be that to meet its UNSCR 1540 physical protection obligation, every state with nuclear weapons or weapons-usable nuclear materials should have a well-enforced national rule requiring that every facility with a nuclear bomb or a significant quantity of nuclear material must have security in place capable of defeating a specified set of insider and outsider threats comparable to those terrorists and criminals have demonstrated in that country (or nearby). This approach has the following advantages: the logic is simple, easy to explain, and difficult to argue against; the standard is general and flexible enough to allow countries to pursue their own specific approaches as long as they are effective enough to meet the threats; and at the same time, it is specific enough to be effective and to provide the basis for questioning, assessment, and review.[30] The United States and

---

[28] The text of UNSCR 1540, along with many related documents, can be found at United Nations, "1540 Committee" (New York: UN, 2005; available at http://disarmament2.un.org/Committee1540/meeting.html as of 25 February 2005).

[29] For discussion, see Matthew Bunn, "UNSC 1540: Next Steps to Seize the Opportunity," paper presented at A New Role for the United Nations Security Council: Criminalizing WMD Proliferation--The Impact of U.N. Security Council Resolution 1540, Arlington, Va., 15 March 2005 (available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/UNSC1540.pdf as of 2 January 2007).

[30] Questions designed to clarify a country's compliance with this standard could include such items as: is there a rule in place specifying that all facilities with nuclear weapons or significant quantities of weapons-usable

other nations agreeing to such a standard should then launch an intensive effort to persuade other states to bring their nuclear security arrangements up to that standard and help them to do so as needed.

The United States should also make clear to all countries where nuclear stockpiles exist that with the passage of UNSCR 1540, providing effective security for these stockpiles is now a legal obligation and a positive relationship with the United States depends on fulfilling that obligation.

Strengthening IAEA recommendations. The current version of the IAEA recommendations on physical protection, INFCIRC/225 Rev. 4, was issued in 1999, long before the 9/11 attacks. As discussed in Chapters 4 and 5, its requirements are quite modest. As of late 2006, international discussions of a fifth revision are expected to begin soon.[31] The United States and other leading governments should see these talks as another opportunity to build toward commonly followed global standards of nuclear security that would be effective enough to reduce the risk posed by potential nuclear theft to a low level.

INFCIRC/225 Rev. 4 already recommends that states develop a DBT and make it an "essential element" of their physical protection systems.[32] But it does not specifiy anything about what the DBT should be or how exactly it should be used. The document is almost

---

nuclear material must have security in place capable of defending against specified insider and outsider threats? Are those specified threats big enough to realistically reflect demonstrated terrorist and criminal capabilities in that country or region? How is this requirement enforced? Is there a program of regular, realistic tests, to demonstrate whether facilities security approaches are in fact able to defeat the specified threats? Are armed guards used on-site at nuclear facilities, and if not, how is the system able to hold off outside attack or insider thieves long enough for armed response forces to arrive from elsewhere? Others have proposed other standards to meet similar objectives: Graham T. Allison, for example, has proposed a "gold standard," arguing that given the devastating potential consequences of nuclear theft, all nuclear stockpiles should be secured to levels similar to those used for large stores of gold such as Fort Knox. See Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*. In 1994, a committee of the National Academy of Sciences argued that because getting the essential ingredients of nuclear weapons was the hardest part of making a nuclear bomb, plutonium should, to the extent practicable, be secured and accounted for to the same standards applied to nuclear weapons themselves – and argued further that this "stored weapon standard" should be applied to all separated plutonium and HEU worldwide (an approach that presupposes that nuclear weapons themselves have effective protection, which may not always be the case). U.S. National Academy of Sciences, Committee on International Security and Arms Control, *Management and Disposition of Excess Weapons Plutonium* (Washington, D.C.: National Academy Press, 1994; available at http://books.nap.edu/html/plutonium/0309050421.pdf as of 30 December 2006), pp. 31, 102. Other sources that could also be drawn on for insight in defining what should be included in an "appropriate effective" physical protection system include the "principles and objectives" included in the proposed amendment to the physical protection convention (though these are very general and include few specifics) and the IAEA's recommendations on physical protection (INFIRC/225 Rev. 4). Unfortunately, while both of these provide valuable considerations for physical protection, it is possible to comply fully with both of them and still not have a secure system.

[31] Interviews with DOE and State Department officials, July 2006 and October 2006; interview with IAEA Office of Nuclear Security official, July 2006. The new version may be renamed – the IAEA hopes to have it as one entry in its new "Security Series" of publications, giving it a status comparable to the status of the "Safety Series" documents, which have become de facto global standards on a variety of aspects of nuclear safety.

[32] International Atomic Energy Agency, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected) (Vienna: IAEA, 1999; available at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html as of 22 December 2006).

entirely rule-based, rather than performance-based. A new revision should move in a more performance-based direction, focused on providing capabilities to meet particular threats. Ideally, a new revision should recommend that: (a) states should enact and enforce regulations that will ensure that all facilities and transport legs with Category I material (at least) have security systems in place able to provide a high probability of defeating the DBT;[33] and (b) that, while DBTs should vary from one state to another depending on the threat, at a minimum all Category I material should be defended at least against a modest group of well-armed and well-trained outsiders (capable of operating as two or more teams), with access to inside information on the workings of the security system and the location of the material, against one or two well-placed insiders, or against both outsiders and insiders working together. Whether or not that level of specificity could be achieved, it would also be useful for a new revision of INFCIRC/225 to specify that the DBT in each state should include at least the level of capabilities that terrorists or thieves stealing from major guarded facilities or transports have demonstrated they can pull together in that state, or in neighboring states with similar threat conditions; this would provide a basis for detailed discussions with states about whether their DBTs adequately reflected the threats they had experienced.

The minimum threat suggested above, if agreed to, would represent a very substantial step forward in the way nuclear material is protected around the world. Most countries comply with the recommendations of INFCIRC/225, either because they choose to follow international guidelines, or because a variety of legal requirements oblige them to (in particular, nuclear supply agreements which often contain a provision requiring that material be protected at least to the levels called for in INFCIRC/225). The minimum DBT just outlined corresponds roughly to the published version of the U.S. NRC DBT for theft.[34] This DBT is less capable than it should be in a variety of respects and is far less capable than the DOE DBT for identical material;[35] but it represents a level of protection well beyond that which exists today at the most vulnerable facilities with HEU and separated plutonium around the world, and it is the most that could reasonably be hoped for (and possibly more than can

---

[33] To gain sufficiently broad support, it may be necessary to include language that makes it clear that states could choose to achieve this level of performance either through a performance-based approach in which facilities are required to be able to defeat a certain DBT but given significant flexibility in how to go about doing so; a rule-based approach in which the regulations specify particular security measures to be taken, in the expectation that if those measures are taken as specified, the result will be a system that provides protection adequate to defeat the DBT; or a combination of performance-based and rule-based approaches. While a number of states have adopted DBT-centered approaches to physical protection regulation, many others have not, and no state has yet adopted an entirely performance-based approach without a substantial number of rule-based requirements.

[34] See Section 73.1 in U.S. Nuclear Regulatory Commission, "Part 73-Physical Protection of Plants and Materials," in *Title 10, Code of Federal Regulations* (Washington, D.C.: U.S. Government Printing Office; available at http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html as of 28 September 2005).

[35] For a more radical argument that INFCIRC/225 should be revised to incorporate a DBT comparable to that now in use at DOE, see Edwin S. Lyman, "Using Bilateral Mechanisms to Strengthen Physical Protection Worldwide," in *Proceedings of the 45th Annual Meeting of the Institute for Nuclear Materials Management, Orlando, Florida, 18-22-July* (Northbrook, Ill.: INMM, 2004; available at http://www.ucsusa.org/global_security/nuclear_terrorism/bilateral-mechanisms.html as of 21 November 2006). Unfortunately, given the system constraints described in Chapter 5, I do not believe that such a far-reaching revision of INFCIRC/225 could be achieved; even the approach described in the text would be a stretch.

actually be achieved) as an agreement resulting from the IAEA's least-common-denominator discussion process.

Because of the likely difficulty of achieving such an objective in that process, the United States should explore this possibility with a number of key like-minded states in advance. If a substantial number of the major states had already reached consensus before the formal discussions at the IAEA began, the chances of getting agreement on such a formal discussions at the IAEA

A variety of other improvements should be made in INFCIRC/225 as well. More measures are needed focused on the insider threat – likely the dominant theft and sabotage threat in many countries – including more specifics on the need for in-depth background checks and ongoing monitoring of personnel, continuous monitoring of areas with Category I nuclear material (and vital areas in the case of sabotage), training to ensure that all personnel are alert to the possibility of insider theft and know how to report any suspicions they may have, and more. The document should recommend that the actual performance of physical protection systems in defeating both outsider and insider threats be regularly probed with realistic tests in which either test participants portraying outsiders attempt to get in and steal material, or participants portraying insiders attempt to remove material. If agreement can be reached, it would be highly desirable for the revised document to specifically call for on-site armed guards numerous and effective enough to be able to defeat the DBT; if some states insist on retaining something like the current language allowing for "compensatory measures" instead of on-site armed guards, this language should be made more specific, recommending that states not allow the substitution of compensatory measures for armed guards unless the compensatory measures have proved, in realistic tests using teams trained in plausible adversary tactics, that they can provide an equivalent level of protection. The points emphasized in the fundamental principles of physical protection in the amendment to the physical protection convention – including, among others, the importance of security culture – should be included in INFCIRC/225, each with specific recommendations as to how they can be addressed. The very brief discussion of measures to prevent sabotage in the current document should be expanded. Finally, as discussed below, the approach to categorizing nuclear material needs to be changed.

New approaches to categorizing nuclear material. As discussed in detail in Chapter 4, existing DOE, NRC, and IAEA approaches to categorizing nuclear material and assigning levels of security for each of the categories should be modified. The United States and other leading governments should adopt categorization tables based on an approach similar to that outlined in Chapter 4. In particular, it is clear that nuclear material emitting 100 rad/hour at one meter is not self-protecting against thieves willing to absorb substantial doses and requires substantial security measures.

It may be difficult to reach agreement on modifying the categorization table in INFCIRC/225, particularly since the identical table is incorporated in the text of the physical protection convention, and no one has the stomach for undertaking another convention amendment in the near term. If it proves unduly difficult to change the table itself, the already-existing language recommending that states provide security for nuclear materials in

proportion to their usability in nuclear explosives could be elaborated and spelled out in more detail; the language indicating that states can reduce the category assigned to nuclear material by one step (for example, from Category I to Category II) if it is emitting 100 rad/hr at one meter (also incorporated in the physical protection convention) could be modified in INFCIRC/225 by adding a recommendation that states should not make this reduction unless compensatory measures were taken to provide equivalent levels of protection against thieves not concerned with their own health.

Tougher export requirements. U.S. law requires that nuclear exports not be "inimical to the common defense and security."[36] To date, with respect to the threat to the common defense and security posed by potential nuclear theft, the United States has implemented this requirement by requiring that states receiving nuclear exports provide security at least equivalent to that called for in the latest IAEA recommendations. U.S. nuclear cooperation agreements with other countries typically reflect these requirements.

But a strong argument can be made that the requirements of INFCIRC/225 Rev. 4 are not sufficient to ensure that exports of weapons-usable nuclear material will not pose a risk of nuclear theft high enough to be inimical to the common defense and security.[37] Existing nuclear cooperation agreements referring only to the IAEA recommendations as the standard of adequacy probably make it impossible for the United States to legally require that holders of U.S.-origin material take measures going far beyond the IAEA recommendations; but there is nothing preventing the United States from launching diplomatic efforts to convince these states that in their own security interests, higher standards of security are needed. Moreover, in compliance with the law, an argument can be made that future exports of HEU or separated plutonium should only be made if they will be handled, as long as they remain in weapons-usable form, with security measures adequate to reduce the risk of nuclear theft and terrorism they pose to very low levels. As suggested above, the United States should take the position that only nuclear facilities with security that has demonstrated high levels of effectiveness can receive U.S. nuclear material or lucrative U.S. government contracts – and should work to convince other leading states to do the same.

In addition, the United States and other leading governments should work to strengthen the guidelines on physical protection of the Nuclear Suppliers Group (NSG). These guidelines, which appear not to have been modified significantly since they were agreed to in 1975, refer to INFCIRC/225 as a "useful basis" for guiding individual states in designing physical protection systems; but the specific measures the NSG members agree to require are considerably weaker than those in INFCIRC/225.[38] More than five years after the 9/11 attacks, it is past time to revise these guidelines so that all major suppliers agree to

---

[36] *Atomic Energy Act of 1954, as Amended* (Washington, D.C.: Government Printing Office, 1954; available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0980/ml022200075-vol1.pdf as of 22 December 2006).

[37] Lyman, "Using Bilateral Mechanisms."

[38] See Appendix C of the NSG guidelines, contained in International Atomic Energy Agency, *Communications Received from Certain Member States Regarding Guidelines for the Export of Nuclear Material, Equipment and Technology*, INFCIRC/254/Rev. 7/Part 1 (Vienna: IAEA, 2005; available at http://www.nuclearsuppliersgroup.org/PDF/infcirc254r7p1-050223.pdf as of 20 July 2005).

require physical protection sufficient to defeat the kinds of threats that terrorists and criminals have shown they can pose. Ultimately, as suggested above, good security must become part of the price of admission for operating in the international nuclear market.

National-level rules. Ultimately, the actual nuclear security measures taken in each state are determined by that state. Hence the principal purpose of international standards, commitments, and recommendations is to influence the nuclear security rules and practices within each state. If it is possible to influence those rules and practices directly, so much the better. The United States and other leading governments should substantially increase the level of diplomatic effort they devote to convincing countries around the world to put in place regulations requiring that every nuclear warhead or significant stock of HEU or separated plutonium on their soil or under their control have security measures that will offer a high probability of defeating the kinds of threats terrorists and criminals have shown they can pose in that country. As discussed above, effective and effectively enforced nuclear security rules are essential to achieving high levels of nuclear security that last for the long haul and should be a fundamental goal of every bilateral effort to upgrade nuclear security.

Recently, for example, the United States has had an extended series of discussions with Japan over physical protection regulations in Japan.[39] Until recently, Japan's regulations were still based on INFCIRC/225 Rev. 3, not Rev. 4, and did not incorporate a DBT. Discussions with the United States (and the requirements of the U.S.-Japan nuclear cooperation agreement) were among the factors that convinced Japan to undertake a substantial revision of its physical protection regulations, requiring facilities to be able to defend against a specified DBT for the first time. As noted in Chapter 4, however, Japanese physical protection arrangements remain much less substantial than those in the United States and a number of other countries, and the actual additional measures taken to comply with the new regulations were modest. This experience demonstrates that U.S. pressure can contribute to positive change but also suggests that more will be needed to convince states to go far enough to reduce the threat to a low level.

In seeking to strengthen national nuclear security rules, the United States should begin with its own. Effective nuclear security rules in the United States are important both to reduce genuine risks within the United States and because it will be extraordinarily difficult to convince other states to strengthen their nuclear security rules in ways that may be expensive or inconvenient if they can readily observe that the United States has not taken similar steps itself. The United States should take all of the following steps:

- NRC and DOE should act in concert to phase out the "interim" exemption from most physical protection requirements that NRC-regulated research reactors were granted almost three decades ago. NRC should change its regulations and DOE, which covers most of the cost of operations at these research reactors, should pay the increased security costs (which will be a tiny addition to what DOE is already paying for security at its own facilities). Regulations should be set so that the probability of a theft attempt being successful at a research reactor is no higher than it is at other NRC-regulated facilities

[39] Interviews with DOE, State Department, and Japanese officials, November 2006.

with HEU of similar quality, taking into account the security measures combined with the inherent characteristics of the facility (such as the difficulty of accessing the HEU in a research reactor pool).

- As discussed in Chapter 4, NRC should abandon its policy of exempting material emitting 100 rem/hr at three feet from virtually all security requirements.
- NRC should modify its requirements for special nuclear material of low and moderate strategic significance, so that the security measures it requires decline in a more graded way as the quality or quantity of nuclear material declines and do not fall off a cliff when particular arbitrary thresholds are reached. (This issue is also addressed in Chapter 4.) In particular, NRC's regulations should comply with the IAEA recommendation that Category II material, like Category I material, should be stored in an area enclosed by a fence with intrusion detection (and with the other IAEA recommendations for Category II material).
- NRC and DOE should also act in concert to bring the NRC DBT for Category I material into line with the DBT that DOE facilities must meet. When DOE and NRC were first established, there was a doctrine of security "comparability" – that is, their security rules for nuclear material need not be identical, but overall, the security measures should be comparable, so that potential thieves would not have a much easier time stealing material under one organization's jurisdiction than under the other's. The rationale for comparability remains extremely strong, but the doctrine has fallen out the window in recent years. The threat that the two major Category I sites regulated by NRC – which handle tons of weapons-grade HEU metal – are required to be protected against is far less than the threat DOE sites are now required to be protected against. Yet here, too, DOE pays most of the costs of operation of these privately-owned facilities, through contracts for their services doing various types of HEU processing. NRC should change its rules for security for Category I sites to make them comparable to the security required at DOE Category I sites, and DOE should agree to pay the costs of meeting these new security requirements at these two facilities.[40]
- NRC should reverse its decision that plutonium-uranium mixed oxide (MOX) fuel poses little theft threat and should require security measures at sites handling Category I quantities of MOX that reduce the overall risk posed by nuclear theft and terrorism to a level comparable to that at other Category I facilities. Such an approach should, however, take into account the risk reduction arising from the material's characteristics, as described in Chapter 4, and therefore the rules could allow security measures that would result in a somewhat higher probability that a theft attempt would be successful than would be allowed for HEU metal.
- DOE should adopt a more realistic approach to categorizing nuclear material for graded safeguards, as described in Chapter 4. (A revision of DOE's categorization approaches is

[40] For a similar suggestion, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006).

under way,[41] but whether it will eliminate all of the aspects of the current categorization approach that are unjustified and should be changed remains to be seen.)

Building confidence in nuclear security. A particularly difficult problem is how to build confidence that nuclear security commitments have been implemented once they have been made. Such confidence is critical, as every country has a direct national security interest in making sure that all countries with nuclear weapons and weapons-usable materials provide effective security for them. But in nearly every country with such stockpiles, the details of nuclear security arrangements are highly classified, making it difficult to reveal enough information to prove that the security measures in place are fully effective.[42]

For those countries willing to accept international peer reviews of their security arrangements, IAEA-led peer reviews can be effective in building confidence. Such peer reviews should increasingly become a normal part of the nuclear business for developed and developing states alike, just as international safety reviews are.[43] But the reality is that some nuclear stockpiles – from those at U.S. and Russian nuclear warhead assembly plants to those in Pakistan and Israel – are extremely unlikely to be welcoming IAEA visitors anytime in the next decade. Graham Allison has proposed that nuclear weapon states invite experts from another nuclear weapon state with which they have good relations to review their nuclear security arrangements and certify that they are effective. China, for example, which has long had close nuclear relations with Pakistan, might review and certify Pakistan's nuclear security system.[44]

Another approach might focus on providing, at least in general terms, the results of tests of security system effectiveness. The United States, for example, already openly publishes data on what percentage of DOE facilities have received high ratings in DOE security inspections – and uses that percentage as a measure of the effectiveness of ongoing steps to improve security.[45] In the case of U.S.-Russian cooperation, to build understanding of what was being tested and how, U.S. and Russian adversary teams used to test the

---

[41] Joseph Rivers and D.L. Whaley, "Review of the Department of Energy Graded Safeguards Table," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).

[42] Even at sites in Russia where the United States has invested heavily in improving security, Russia does not inform the United States about operational details of day-to-day security measures important to the effectiveness of the overall system; and the United States has given Russia very little information about the day-to-day effectiveness of U.S. nuclear security systems.

[43] Norway was the first major developed state to request such an international peer review and encouraged all other states to do likewise, arguing that all states can benefit from international advice. Government of Norway, "Statement by Norway," in *48th IAEA General Conference, Vienna, Austria, 20-21 September 2004* (Vienna: International Atomic Energy Agency, 2004; available at http://www.iaea.org/About/Policy/GC/GC48/Statements/norway.pdf as of 10 May 2006).

[44] Allison, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, pp. 150-153.

[45] See, for example, U.S. Department of Energy, *FY 2006 Congressional Budget Request: National Nuclear Security Administration* (Washington, D.C.: DOE, 2005; available at http://www.cfo.doe.gov/budget/06budget/Content/Volumes/Vol_1_NNSA.pdf as of 18 July 2005), pp. 416-419. Note that in fiscal 2004, the last year whose actual results are reported here, DOE inspectors had rated the security at individual sites "effective" in only 53% of their inspections – and the targets for fiscal 2005 and fiscal 2006 were only to achieve 65% and 70% "effective" ratings, respectively.

effectiveness of nuclear security systems against outsider and insider threats might train together and perhaps conduct tests with joint U.S.-Russian teams at one or two non-sensitive sites in each country. Then the remaining sites could be tested by purely national teams, using similar approaches and standards, and broad descriptions of the results could be provided to the other country. In the case of tests that revealed vulnerabilities requiring immediate corrective action, U.S. and Russian officials would probably not want to reveal the specifics of those vulnerabilities to the other side until they had been corrected; the existence of such vulnerabilities is considered a secret in each country. In cases where deficiencies were found, they could simply be silent about the results of the test, leaving the other side to draw its own conclusions, until after corrective action had been completed. Such an approach could provide substantially increased confidence to each side that the other's nuclear stockpiles were secure and were being tested effectively. In particular, an approach like this one might be used to confirm that Russia had taken action to provide security at sites that had been judged too sensitive to allow U.S. access that was comparable to the security measures at sites where U.S.-Russian cooperation had taken place, particularly the two remaining nuclear warhead assembly and disassembly facilities.

Approaches such as these are sensible goals to aim for, though they will be extremely difficult to achieve. In the immediate term, states should do more to provide general descriptions of their nuclear security approaches, photographs of installed equipment, and related data that could be made public without providing data that could help terrorists and criminals plan their attacks.

Strengthening the Nuclear Security Role of the IAEA

The IAEA Office of Nuclear Security, established in its current form in the wake of the 9/11 attacks, can play a crucial role in helping to set standards and disseminate best practices for nuclear security, in providing training, in assessing countries' needs, and in coordinating nuclear security assistance to countries around the world. In many countries, assessment teams and assistance organized by the IAEA would be far more welcome than U.S. assessment and assistance. With UNSCR 1540, there are now scores of countries that may require assistance to meet the binding legal obligations to provide effective nuclear security that they now face. Yet the Office of Nuclear Security has so far labored with an extraordinarily small staff and a tiny budget (expected to average in the range of $15 million per year over the next several years – while the cost of substantially upgrading security at one site often exceeds $10 million).

The United States should work with other leading governments to expand the mission, personnel, and resources of the Office of Nuclear Security, allowing the IAEA to substantially increase its contribution to preventing nuclear terrorism. Specifically, this office should be given the resources to perform larger numbers of more in-depth nuclear vulnerability assessments and other evaluations of needs for prevention of nuclear terrorism. It should have a small fund for actually paying to implement needed security upgrades (possibly a rotating fund to be replenished by donor states when expended) so that when IAEA-organized reviews identify an urgent need for security upgrades, these can be implemented immediately without waiting to negotiate new agreements with donor states to provide the necessary assistance.

The Office of Nuclear Security should also be given the mission and resources to take a leading role in assessing states' needs and coordinating assistance that would help them comply with the nuclear provisions of UNSCR 1540. This office can also play a key role in identifying and promoting best practices in nuclear security and organizing international best-practice discussions; it should be given the resources and mandate to do so. Finally, the Office of Nuclear Security manages the main global database on nuclear smuggling, but has few resources available to analyze cases in depth and provide lessons learned to member states; an IAEA-led effort to analyze not only nuclear smuggling cases but cases of terrorist attacks and criminal thefts from guarded facilities worldwide, in order to identify the types of adversary capabilities that nuclear sites should be prepared to defend against, could be extremely important. The budget of the Office of Nuclear Security should be increased to at least the range of $30-$50 million, and most of the office's budget should become part of the IAEA's regular assessed budget, rather than relying entirely on voluntary contributions.

An Industry Nuclear Security Initiative

In addition to governments, the nuclear industry itself has a major role to play in forging effective global nuclear security standards and exchanging best practices for achieving high levels of security. A new Chernobyl caused by a terrorist sabotage, or worse yet a city being destroyed by a terrorist nuclear bomb, would not only cause catastrophic damage and human suffering, it would also be a political disaster of epic proportions for the nuclear industry, spelling the end of any realistic prospect that nuclear energy could be expanded to deal with the challenge of climate change. Hence, just as in the case of safety, industry has a strong self-interest in helping those facilities with the worst security performance reach the standards of the top performers. The nuclear industry should take the lead, launching a World Institute of Nuclear Security (WINS) – modeled in some respects on the World Association of Nuclear Operators (WANO), which has played a key role in improving nuclear safety around the world – which would develop standards, exchange and circulate best practices, perform industry peer reviews and other advisory services on request, and more. Just as has been the case with WANO's role in nuclear safety, such an industry-led effort could effectively complement (rather than undermine) related ongoing work being done by the IAEA and by national governments. The Nuclear Threat Initiative (NTI) has challenged the Institute for Nuclear Materials Management (INMM) to play a central role in launching such an initiative.[46] In response, a team of INMM experts developed a more detailed concept of how such an organization might function, and several stakeholders are now working to develop the concept in more detail.

To ensure that such an initiative has the necessary clout, it will be important to develop it in a way that maximizes industry buy-in, particularly from those controlling the purse-strings. What made WANO and its U.S.-based predecessor, the Institute of Nuclear Power Operations (INPO), so effective was that the industry perceived them as its own ideas, operating to serve the industry's own interest. These organizations also had direct access to

---

[46] Charles Curtis, "Promoting Global Best Practices," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005; available at http://www.nti.org/c_press/speech_curtisINMM_071105.pdf as of 8 June 2006).

the utility CEOs, who could bring powerful peer pressure to bear on any CEO whose utility was lagging behind.[47]

An Accelerated Global Cleanout

Nuclear security improvements only reduce risks; they can never eliminate them. The only foolproof way to ensure that nuclear material will not be stolen from a particular site is to remove it. The United States and other leading governments need to work together to accelerate and broaden to consolidate both nuclear weapons and weapons-usable nuclear materials at the smallest practicable number of sites, achieving higher security at lower cost. This effort should focus particularly on removing material from the highest-risk sites – sites that are especially vulnerable and difficult to defend, and sites in especially high-threat countries.

The Global Threat Reduction Initiative (GTRI), launched in the spring of 2004, was established to accomplish that goal – but there is still much to be done to accelerate and strengthen that effort.[48] The goal should be to remove the weapons-usable nuclear material entirely from the world's highest-risk, least defensible sites within four years – substantially upgrading security wherever that cannot be accomplished – and to eliminate all HEU from civil sites worldwide within roughly a decade.[49] The United States should make every effort to build international consensus that the civilian use of HEU is no longer acceptable, that all HEU should be removed from all civilian sites, and that all civilian commerce in HEU should brought to an end as quickly as possible.[50]

The global coalition described above should seek: to close and decommission HEU-fueled research reactors and other sites with HEU or separated plutonium that are no longer needed; to accelerate conversion of HEU or plutonium-fueled research reactors that will continue to operate and for which replacement low-enriched uranium (LEU) fuel is available; to assure that fuels are developed as soon as possible to convert all or nearly all of the remaining still-needed research reactors; and to ensure that effective security is in place (meeting global standards such as those described above) and that both the on-site inventories

---

[47] For a fascinating discussion of INPO, its record of effectiveness, and the factors that caused that outcome, see Joseph V. Rees, *Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island* (Chicago: University of Chicago, 1996).

[48] GTRI also addresses radiological materials that could be used in a so-called "dirty bomb," both within the United States and internationally. That important topic is not the subject of this dissertation, however.

[49] In saying that all the HEU should be removed from the world's most vulnerable sites within four years – a recommendation I have been making for several years – I am *not* suggesting that it is possible to convert every HEU-fueled research reactor within four years. Rather, the argument is that all HEU should be removed from those sites identified as having both (a) enough HEU for a nuclear bomb, and (b) inadequate security to meet the threats they face, within that time. In some cases, this may mean encouraging reactors that are no longer needed to shut down rather than converting; where neither conversion nor shut-down is realistically possible in a short time span, substantial security upgrades need to be put in place rapidly, sufficient to remove the site from the list of the world's most vulnerable facilities.

[50] For a similar recommendation, see Charles Ferguson, *Preventing Catastrophic Nuclear Terrorism* (Washington, D.C.: Council on Foreign Relations, 2006; available at http://www.cfr.org/content/publications/attachments/NucTerrCSR.pdf as of 8 June 2006).

of HEU and the enrichment of HEU are minimized, for those sites where all the HEU cannot be removed immediately.[51]

Success in achieving these goals will require focusing comprehensively on *all* the facilities that have vulnerable potential nuclear bomb material, not just those that happen to be operating civilian research reactors, or whose nuclear material happens to be Russian-supplied or U.S. supplied. Success will require flexible and creative tactics, with approaches – including incentives to give up the nuclear material – targeted to the needs of each facility and host country. It will also require the United States to convert and adequately secure its own HEU-fueled research reactors, not only to remove such threats from inside U.S. borders but also to enable U.S. leadership in convincing others to do the same.

A comprehensive approach. GTRI was explicitly intended to take a comprehensive approach to the problem of insecure nuclear material around the world. GTRI has established an "emerging threats" sub-program which is intended to cover what GTRI refers to as "gap materials" – those materials that fell through the cracks in pre-existing programs. To its credit, DOE has prepared and revised a list of the facilities around the world where weapons-usable nuclear materials exist, to provide the basis for a comprehensive approach, though DOE officials report that as further visits to particular sites are conducted, new facilities using HEU are still being identified.[52]

But major gaps remain:

- Some twelve tons of U.S.-origin HEU in foreign countries is not covered by the current U.S. take-back offer; this represents some two-thirds of the U.S.-origin HEU that was still abroad when the take-back offer was renewed in 1996. While most of this material is in Germany, France, the United Kingdom, or Japan, significant quantities are not, and even in advanced countries HEU at research reactors is often protected in a way that still leaves a significant remaining risk of nuclear theft.
- Many HEU-fueled reactors are not yet slated for conversion to low-enriched uranium (LEU) fuel or shut-down. In particular, a very large fraction of the world's critical assemblies and pulse reactors, which often have huge quantities of weapons-usable material on-site, are not yet slated for conversion or shut-down. Similarly, most producers of medical isotopes using HEU targets have strongly resisted conversion to LEU. Some HEU-fueled reactor types not yet covered by GTRI at all, such as icebreaker and submarine reactors.

---

[51] A similar listing of steps was first proposed in International Panel on Fissile Materials, *Global Fissile Material 2006: Report of the International Panel on Fissile Materials* (Princeton, N.J.: Program on Science and Global Security, Princeton University, 2006; available at http://www.fissilematerials.org/ipfm/site_down/ipfmreport06.pdf as of 24 January 2007).

[52] Interviews with DOE officials, February, April, and December 2005.

- Similarly, some HEU does not come from either the United States or Russia and hence is not covered by either the U.S. or Russian fuel take-back efforts – though in some cases such material may be addressed by the "gap materials" effort.[53]

A creative and flexible set of tactics for addressing the problem. Rapidly convincing facilities and countries all over the world to stop using potential nuclear bomb material and allow the material they have to be removed will be an immense challenge. The task will require considerable tactical creativity, flexibility, and perseverance. Several additions to the set of policy tools currently being applied to the problem seem likely to be essential:

- *Packages of incentives targeted to the needs of each country or facility.* Substantial incentives will be needed to convince the operators of research reactors to convert their facilities to LEU (or shut them down) and give up their HEU.[54] The United States and its international partners should offer packages of incentives that make it unambiguously in the interest of the facility or the country that operates it to get rid of the HEU at vulnerable sites. Such packages could include help with converting to LEU; help with improvements that would make the reactor function even better after conversion than before; help with shutting and decommissioning a reactor; contracts for other research by the scientists at a site after agreement is reached to shut the site's reactor, including shared use of reactors at other sites; help with managing the wastes from a research reactor; and other steps, many of which will not even be thought of until a particular case arises.[55] It appears that additional incentives are also likely to be needed to convince facilities to return even that portion of the U.S.-supplied HEU abroad that is covered by the current U.S. take-back offer.[56]

---

[53] Matthew Bunn and Anthony Wier, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 2 January 2007). See also Alexander Glaser and Frank N. von Hippel, "Global Cleanout: Reducing the Threat of HEU-Fueled Nuclear Terrorism," *Arms Control Today* (January/February 2006; available at http://www.armscontrol.org/act/2006_01-02/JANFEB-heuFeature.asp as of 8 June 2006); Frank von Hippel, "A Comprehensive Approach to Elimination of Highly-Enriched Uranium from All Nuclear Reactor-Reactor Fuel Cycles," *Science and Global Security* 12, no. 3 (November 2004).

[54] For a discussion of some of the incentives packages that worked in past cases of HEU removals, see Philipp C. Bleek, *Global Cleanout: An Emerging Approach to the Civil Nuclear Material Threat* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2004; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/bleekglobalcleanout.pdf as of 13 April 2005).

[55] Where necessary, this should include help paying for the cost of new LEU fuel (especially in cases were reactor otherwise would not buy new LEU fuel because it already has HEU that will last for many years, or for the lifetime of the reactor).

[56] U.S. Congress, Government Accountability Office, *Nuclear Nonproliferation: DOE Needs to Consider Options to Accelerate the Return of Weapons-Usable Uranium from Other Countries to the United States and Russia*, GAO-05-57 (Washington, D.C.: GAO, 2004; available at http://www.gao.gov/new.items/d0557.pdf as of 2 February 2005). Putting together such packages of incentives will require some broadening of current thinking and an expansion of current budgets (which do not include any funding for incentives going beyond paying the costs of conversion to LEU). Currently, for example, GTRI is willing to help research reactors convert to LEU, so that conversion does not represent a substantial new cost to the reactor operator – but it is generally not

- *Providing incentives for shutting HEU-fueled reactors, in addition to conversion.* Most of the world's research reactors are aging and unneeded. The best answer for many of them is to provide incentives to shut them down. Unlike conversion, shut-down need not wait for the development of new fuels; it can be pursued immediately. For most of the dozens of HEU-fueled research reactors not currently on the target list for conversion (and for many of those that are), the shut-down option would be quicker, less costly, and more likely to succeed than conversion. There is good evidence that such an approach can work, as even in the absence of any effort to provide shut-down incentives, far more HEU-fueled reactors have shut down since 1978, when the effort to convert reactors to LEU began, than have successfully converted.[57] Indeed, IAEA experts have estimated that of the more than 270 research reactors still operating in the world (both HEU-fueled and otherwise), only 30-40 are likely to be needed in the long term.[58] No research reactor operator wants to shut his or her facility. Convincing sites to shut down their reactors is likely to require substantial packages of incentives. In some cases, the best route will be through national governments, which may be growing tired of the drain on the budget imposed by subsidizing these reactors and may be more willing to negotiate over these reactors' fate than the operators themselves. Considerable care will be needed to avoid having the efforts of officials seeking to build trust with reactor operators to convince them to convert to LEU contaminated by suspicion that the real agenda is to shut these reactors down.[59]
- *Security upgrades and strengthened security rules, in concert with material removals.* As weapons-usable nuclear material cannot be removed from the world's most vulnerable sites overnight, security should be upgraded at these sites for the period before material is removed. Through GTRI or whatever other rubric is most appropriate, the United States

---

willing to make research reactors *better* off than they were before conversion, even if doing so would carry modest cost while being crucial to gaining agreement to convert. This policy should be reversed. GTRI program managers do not want to drive up the price that reactor operators demand for their cooperation, and that is a legitimate issue. But within reason, price should not be allowed to stand in the way of success. U.S. taxpayers would be better served by an $800 million cleanout effort that succeeded in convincing all of the world's most vulnerable sites to give up their weapons-usable material than they would by a $400 million effort that left dozens of vulnerable sites with HEU still in place.

[57] Iain Ritchie, "IAEA Presentation on Threat Reduction Activities," paper presented at The Global Threat Reduction Initiative International Partners' Conference, Vienna, Austria, 18-19 September 2004.

[58] International Atomic Energy Agency, "New Life for Research Reactors? Bright Future but Far Fewer Projected" (Vienna: IAEA, 8 March 2004; available at http://www.iaea.org/NewsCenter/Features/ResearchReactors/reactors20040308.html as of 5 January 2007).

[59] No approach perceived by the world's reactor operators as anti-science or anti-nuclear is likely to succeed. Indeed, it is quite possible that such an effort should be undertaken separately from the conversion effort, so that those pursuing conversion will not be "tainted" in the minds of research reactor operators as people seeking to shut them down. As part of such an effort, the international community should help establish a smaller number of more broadly shared research reactors – the same direction that high-energy particle accelerators went long ago. Scientists at sites whose reactors are shutting down should be given funding and access to conduct experiments at other reactors (as is already routinely done in many countries). The best approach might be for the United States and other interested countries to work with the IAEA to launch an IAEA-led "Sound Nuclear Science Initiative," the goal of which would be to get the best science at the lowest cost by getting the research, testing, training, and isotope production the world needs from the minimum number of research reactors.

should assist countries around the world in strengthening security at small, vulnerable sites with weapons-usable nuclear material, and should work with states to put in place nuclear security rules requiring that every facility with significant quantities of weapons-usable material on hand have security measures that are not only enough to comply with the recommendations of INFCIRC/225 Rev. 4 but are sufficient to defeat plausible terrorist and criminal threats. (The cost of complying with such regulations will provide a strong incentive to facilities to eliminate the nuclear material they have on hand; hence, the global cleanout and global nuclear security upgrade agendas go hand-in-hand.) In particular, those remaining research reactors that are still genuinely needed and cannot convert to available LEU fuels without a substantial degradation of their scientific performance should be effectively secured for now and given incentives to convert when development of new, higher-density LEU fuels is completed – which is not likely to occur until early in the next decade.

- *High-level, high-priority diplomacy.* In the past, conversion of research reactors to LEU and removal of HEU from vulnerable sites, have in most cases been handled by program managers and technical experts, not by cabinet or subcabinet national security officials. They have been treated, in essence, as "nice to do" nonproliferation initiatives, not as urgent national security priorities deserving of attention from the highest levels. In part as a result, discussions with many reactors around the world have dragged on for years, often with the hope that agreement to convert the reactor is just around the corner, but with the final deal never quite getting done. If the United States is now to succeed in drastically increasing the pace of HEU removals around the world, the issue will likely need to be on the agenda of senior officials, as one critical element of the global effort to keep nuclear bomb material out of terrorist hands and therefore a high priority for U.S. diplomacy.

Conversion and shut-down in the United States. If the United States wants to convince other countries to convert their research reactors to use fuels that cannot be used in nuclear weapons, to put rules in place requiring high security for those facilities where HEU is still present, and to ensure stringent security for all potential nuclear bomb material, whether in military or in civilian use, it needs to be willing to do the same itself. In particular, the United States should convert all U.S. HEU-fueled research reactors to LEU as soon as possible – a worthwhile move on its own, but also one likely to be an essential element of convincing foreign reactors to convert. If the United States is unwilling to phase out its own civilian use of HEU and provide stringent security for all uses of HEU and separated plutonium, there is little likelihood that it will be able to convince others to do so. Fortunately, in recent years the United States has begun to take important steps in this direction: the research reactors at Texas A&M and Florida State universities were converted to LEU in the fall of 2006,[60] the critical experiments using HEU and plutonium once located at the difficult-to-defend TA-18 site at Los Alamos have been relocated to the secure Device

[60] U.S. Department of Energy, "GTRI: Two Successful Years of Reducing Nuclear Threats" (Washington, D.C.: DOE, May 2006; available at http://www.nnsa.doe.gov/docs/factsheets/2006/NA-06-FS04.pdf as of 21 June 2006).

Assembly Facility in Nevada,[61] and the pulse reactor at Sandia, fueled with a large quantity of HEU, is being shut down.[62] A major effort to consolidate weapons-usable nuclear material to a small number of secure sites is now underway within DOE, intended in large part to achieve better security at lower costs.[63]

Consolidation and security for civilian plutonium. In addition to addressing civilian HEU, the proliferation risks of separated plutonium must be addressed as well. Small quantities of separated plutonium associated with research activities around the world should be addressed by GTRI, removing material from vulnerable sites wherever possible and ensuring that materials that remain are effectively secured.

But plutonium is in civil use on a far larger scale than HEU; it is not just a matter of kilograms or tens of kilograms at research facilities, but tens of tons being separated, stored, processed, and used around the world as fuel for large power reactors. As discussed in Chapter 4, this material is weapons-usable, and it is essential that security and accounting commensurate with post–9/11 threats be maintained throughout all stages of that process. The large investments in plutonium separation facilities that have already been made make it unlikely that proposals for an immediate moratorium on plutonium reprocessing will be adopted.[64] But the Bush administration should do what it can to discourage the spread of civilian separation and use of separated plutonium and should renew the effort to negotiate a U.S.-Russian moratorium on separating weapons-usable plutonium (a 20-year moratorium was nearly agreed at the end of the Clinton administration, which would have ended the accumulation of over a ton of weapons-usable separated plutonium each year at Mayak). Ensuring that plutonium gets security commensurate with the risks it poses should be a high priority throughout all stages of reprocessing, storage, transport, processing, and use. Over the long term, civilian use of separated plutonium should be phased out, in favor of fuel cycles that do not use weapons-usable separated plutonium.

In announcing its proposed Global Nuclear Energy Partnership (GNEP), which it hopes will ease nuclear waste management and thus contribute to the growth of nuclear energy, the Bush administration agreed that traditional reprocessing approaches that fully separate plutonium pose substantial proliferation risks.[65] The Bush administration argues that

---

[61] U.S. Department of Energy, National Nuclear Security Administration, "Sensitive Nuclear Material out of Los Alamos TA-18 Facility" (Washington, D.C.: NNSA, 2 November 2005; available at http://www.nnsa.doe.gov/docs/newsreleases/2005/PR_2005-11-02_NA-05-27.pdf as of 26 December 2006).

[62] Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities.*

[63] For a discussion arguing that substantially more still can and should be done at DOE, see Project on Government Oversight, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities.*

[64] For one such proposal, see Perkovich et al., *Universal Compliance: A Strategy for Nuclear Security.*

[65] Specifically, U.S. Secretary of Energy Samuel Bodman stated, "we all would agree that the stores of plutonium that have built up as a consequence of conventional reprocessing technologies pose a growing proliferation risk that requires vigilant attention." See Samuel Bodman, "Carnegie Endowment for International Peace Moscow Center: Remarks as Prepared for Secretary Bodman" (Moscow: U.S. Department of Energy, 16 March 2006; available at http://energy.gov/news/3348.htm as of 29 December 2006). Critics argue that the waste management approaches proposed in GNEP will undermine rather than promote the future of nuclear energy, asserting that the future of nuclear energy will be brightest if it is made as cheap, simple, safe, proliferation-resistant, and terrorism-resistant as possible, and that reprocessing using past technologies or those

its proposed new approach, known as UREX+, would be proliferation-resistant, since plutonium would not be separated in pure form but would remain with some of the higher actinides and perhaps the lanthanide fission products as well. Unfortunately, however, studies have suggested that this would offer only a very modest proliferation-resistance benefit.[66] And it seems very likely that a decision by the United States, with the largest number of nuclear power plants in the world, to move toward reprocessing will make it more difficult to convince states such as South Korea and Taiwan not to do likewise. (The administration argues that by building a commercial consortium that would offer guaranteed fresh fuel and spent fuel management to countries willing to forego enrichment and reprocessing facilities of their own, they will reduce, not increase, the incentives for countries to build their own reprocessing plants. This is a promising approach, but it does not require reprocessing in the United States, which seems much more likely to convince other states to consider reprocessing than to convince them not to do so.)

Consolidation for both civilian and military nuclear materials. In the United States, DOE has already substantially reduced the costs of guarding plutonium and HEU by closing major sites such as Rocky Flats and greatly reducing the number of buildings with potential bomb material at other sites. Similarly, since the early 1970s, the number of U.S. civilian facilities with licenses to manage Category I quantities of nuclear material has declined dramatically, as the security requirements for such material have increased and prospects for its commercial use have declined. As just noted, DOE is attempting a substantial further reduction in the number of sites and buildings where its weapons-usable nuclear material is located.

Similar efforts to consolidate both military and civilian stockpiles of nuclear material should be made in other countries. Russia, in particular, still has the world's largest nuclear complex, with weapons-usable nuclear materials believed to exist in well over 200 buildings at scores of sites and nuclear warheads believed to exist in well over a hundred bunkers (and a large number of temporary warhead transport or warhead handling areas) at scores of additional sites. While a small number of sites and buildings that once had weapons-usable nuclear material have been cleared out, overall, Russia's progress in consolidating this complex has been modest. The United States should work with Russia to lay out approaches to accomplishing the post-Cold War missions of both countries' nuclear weapons complexes with the smallest possible number of sites and buildings still containing nuclear materials. Russia should stop resisting such consolidation and undertake a focused effort to identify facilities that no longer need HEU or plutonium and encourage or force them to allow their nuclear material to be removed. Large-scale consolidation would greatly reduce the costs of maintaining high levels of security for the long haul and increase the odds that effective

---

proposed in GNEP points in the wrong direction on every count. See, for example, testimony of Matthew Bunn in Committee on Appropriations, Subcommittee on Energy and Water, *Global Nuclear Energy Partnership*, U.S. Senate, 109th Congress, 2nd Session, 14 September 2006.

[66] Jungmin Kang and Frank Von Hippel, "Limited Proliferation-Resistance Benefits from Recycling Unseparated Transuranics and Lanthanides from Light-Water Reactor Spent Fuel," *Science and Global Security* 13, no. 3 (2005).

security will be sustained. On a much smaller scale, there are probably opportunities for such consolidation in countries such as China, France, Britain, Japan, and Germany as well.

Consolidation for nuclear warheads. As discussed in Chapter 2, both the United States and Russia have substantially reduced the number of sites (and countries) where their nuclear weapons exist since the late 1980s. More remains to be done, however. In Russia in particular, there is no reason whatever why nuclear weapons need to remain at scores of separate sites (in addition to those on deployed strategic missiles); leaving the warheads in these vast number of locations would greatly increase long-term security costs and risks. The United States should work with Russia to consolidate warheads at a much smaller number of locations.[67] If existing storage facilities at a small number of sites do not have sufficient capacity to receive warheads from other sites,[68] simple but highly secure bunkers for large numbers of warheads, such as those at the U.S. Pantex facility, could be built in one to two years.

Beyond Improving Nuclear Security

In this dissertation, I have focused primarily on improving security for nuclear stockpiles, as this appears to be the point on the path to nuclear terrorism where policy intervention can have its greatest leverage. The countries that possess nuclear weapons and materials know where they are and can take action to secure them effectively if they have the ability and motivation to do so: the key policy problem is to find ways to provide both ability and motivation where needed. Intervening earlier on the pathway requires successes in detecting and disrupting highly secretive terrorist activities, or in addressing the factors that allow terrorist groups to recruit the kind of people and get the kinds of resources required for a nuclear effort. Intervening later on the pathway is an even greater challenge, as, once stolen, nuclear weapons or materials could be anywhere, and all the things that might be done to find and recover them, or prevent their use, are variations on looking for needles in haystacks. Nonetheless, because efforts to lock down nuclear stockpiles around the world are not likely to be 100% successful – and because some undetected thefts of nuclear material may already have occurred – some investment in other lines of defense is important as well.

Counter-terrorism Efforts Focused on Nuclear Risks

As shown in Chapter 3, counter-terrorist efforts that succeeded in both reducing the number of groups that could plausibly pursue nuclear terrorism and the effectiveness of the remaining ones could substantially reduce the risk of nuclear terrorism, even if they were only

---

[67] For similar recommendations, see Harold P. Smith, Jr., "Consolidating Threat Reduction," *Arms Control Today* 33, no. 9 (November 2003; available at http://www.armscontrol.org/act/2003_11/Smith.asp as of 22 March 2005), p. 19; Gunnar Arbman and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part II: Technical Issues and Policy Recommendations*, vol. FOI-R—1588—SE (Stockholm: Swedish Defense Research Agency, 2005; available at http://www.foi.se/upload/pdf/FOI-RussiasTacticalNuclearWeapons.pdf as of 12 April 2005).

[68] For a discussion of storage capacity constraints as of the late-1990s, see Joshua Handler, *Russian Nuclear Warhead Dismantlement Rates and Storage Site Capacity: Implications for the Implementation of START II and De-Alerting Initiatives*, AC-99-01 (Princeton, N.J.: Center for Energy and Environmental Studies, Princeton University, 1999).

partly successful. The United States and other leading governments should focus substantial efforts on identifying and destroying terrorist groups with the combination of extreme objectives, propensity to mass violence, and substantial financial and technical capabilities that might make them plausible candidates for nuclear terrorism. They should also make a determined effort to identify and track possible observable indicators of nuclear weapons activities – not only statements about nuclear matters and explicit attempts to get nuclear material or expertise,[69] but related activities such as the purchase of induction furnaces and high-temperature crucibles suitable for casting uranium or plutonium, training in shaped explosives suitable for explosive lenses, suspicious chemical leaks or fires, and more.[70]

Terrorist efforts to recruit people with relevant expertise – such as nuclear physicists or metallurgists – may be one of the more detectable activities associated with a nuclear weapons effort. Police and intelligence agencies should seek to build relationships at locations that may pose particular risks of such recruiting efforts, such as technical universities in countries such as Pakistan or Egypt, or universities elsewhere in the world with a substantial number of students from Islamic diaspora, to increase awareness of this potential problem. They should widely disseminate information on easy and anonymous ways to report on any suspicious activities (coupled with a program of rewards for doing so).

Since such activities could occur anywhere in the world, a sustained nuclear counter-terrorism effort cannot succeed without a substantially increased effort to cooperate with intelligence and police services around the world toward these objectives – including improving other countries' efforts (and ability) to monitor indicators of terrorist nuclear interest and activity.

While a terrorist nuclear bomb assembly effort would not require large fixed facilities and might well take place in a developed country, it seems clear that a terrorist-dominated failed state such as the Taliban's Afghanistan offers an even greater ability to work uninterrupted at fixed facilities for prolonged periods, increasing terrorists' chances of success in a nuclear effort. It would be effectively impossible to detect most indicators of such an effort taking place in such a state. Hence, another focus of efforts to reduce the risk of nuclear terrorism should be on efforts to rebuild failed states (including devoting greater resources to preventing Afghanistan from sliding back in that direction), avoid future failed states, and help countries gain control over "stateless zones."

The United States and other leading governments should also work closely with governments that have nuclear stockpiles and face severe threats from terrorists and thieves – such as Russia and Pakistan – to attempt to reduce the scale of those threats. Tougher screening and monitoring of nuclear insiders, anti-corruption programs focused on the nuclear

---

[69] It would be useful, as just one example, to track purchases of books such as *The Los Alamos Primer* and views of particularly informative websites by individuals in countries with active terrorist organizations, or by individuals on relevant watch lists.

[70] For an unclassified summary of a classified study on the prospects for improving capabilities to detect such indicators (which is much more optimistic on the subject than I am), see Michael V. Hynes, John E. Peters, and Joel Kvitky, "Denying Armageddon," *Annals of the American Academy of Political and Social Science* 607 (September 2006).

complex, cooperation to improve government capabilities to detect and stop large-scale conspiracies before attacks occur, and efforts to change the conditions that allow terrorist groups to thrive in these countries could significantly reduce the probability that terrorists or thieves would be able to put together sufficient capabilities to overcome upgraded nuclear security systems and carry out a successful nuclear theft. In other words, efforts to reduce the probability of nuclear theft should focus not only on upgrading the defense but also on reducing the threat.

At the same time, it is worth making a major effort to change the conditions that make it easier for extreme Islamist terrorist groups to recruit and raise funds – to reduce the dangers of all forms of terrorism, not just nuclear terrorism.[71] If the hatred of the United States and the West and the tolerance for terrorism that have become distressingly common commonplace in much of the Islamic world could be changed, through a combination of changes in policies and more effective engagement with the moderate Islamic world, it would have little effect on people who are already hard-core terrorists, but it might significantly undermine their ability to put together the sophisticated technical expertise and substantial resources needed for a nuclear weapons effort. A last resolution of the Israeli-Palestinian conflict, an end to the U.S. domination of Iraq, and consistent efforts seen as contributing to justice and development in the Islamic world could potentially do a great deal to counter the hatred that creates fertile ground for terrorist recruitment and fundraising.

In particular, a targeted discussion of the moral illegitimacy of mass violence on a nuclear scale under Islamic law and other religious traditions – coupled with providing detailed information on just how horrifying the effects of nuclear weapons truly are – could make it more difficult for those terrorists wanting to pursue nuclear violence to convince the people they need to join their cause. After 9/11, bin Laden spent a great deal of his public statements justifying the mass slaughter of innocents (including some Muslims) as legitimate under the circumstances, in response to criticisms from prominent Islamic scholars that this was forbidden under Islamic law; awareness of such concerns may have been what provoked bin Laden to seek a *fatwa* from a radical Saudi cleric holding that the use of nuclear weapons against U.S. citizens was permissible (discussed in Chapter 2). Convincing many of the audiences that al Qaeda plays to that the use of weapons of mass destruction against civilians is a crime that cannot be justified under any circumstances might do as much to reduce the danger of nuclear terrorism as any other step. It would be particularly worthwhile to engage such a discussion at the places where the physicists and metallurgists for a bomb program are most likely to be recruited – at nuclear facilities and universities in countries with sophisticated terrorist groups, with Pakistan at the top of the list.

---

[71] The effort to "diminish the conditions" that lead to terrorism is one of the key elements of U.S. counter-terrorism strategy, but as has been widely noted, it is the one where the United States has been least successful. See, for example, discussion in Bruce Hoffman, *Does Our Counter-Terrorism Strategy Match the Threat?* CT-250-1 (Santa Monica, Calif.: RAND, 2005; available at http://www.rand.org/pubs/testimonies/2005/RAND_CT250-1.pdf as of 28 December 2006). For the beginnings of a set of recommendations for changing this, see, for example, Daniel Benjamin and Steven Simon, *The Next Attack: The Failure of the War on Terror and a Strategy for Getting It Right* (New York: Times Books, 2005).

Reducing the Risk of Nuclear Transfers to Terrorists by States

As discussed in Chapter 3, deliberate decisions by hostile states to provide nuclear bomb materials to terrorists are probably a smaller part of the danger of nuclear terrorism than nuclear theft, because regimes focused on their own survival know that any such act would risk overwhelming retaliation. Nevertheless, steps should be taken to reduce this element of the risk of nuclear terrorism as well. The United States should seek to reduce this risk through a combination of deterrence, disarmament, and efforts to make such transfers more difficult to carry out. The United States should make clear that it will treat any terrorist nuclear attack using a weapon or material provided by a state as an attack by that state and respond accordingly – and should emphasize publicly that it is making every effort to improve its capability to attribute the source of nuclear material in such an event.[72] The United States should also abandon its reluctance to engage directly with Iran and its reluctance to offer serious incentives to North Korea, working with other leading governments to gain international agreement on packages of carrots and sticks large and credible enough to convince Iran and North Korea that it is in their interests to verifiably abandon their nuclear weapons efforts. (Given the events of 2006, including North Korea's partly successful nuclear test and Iran's continued progress toward mastering centrifuges, the prospects for success in this endeavor are now substantially lower than they once were – though the February 2007 agreement with North Korea represents at least a first step in the right direction.) The United States and other leading governments should also take steps to ensure that states in a position to make such transfers do not become sufficiently desperate that such transfers might be seen either as the last chance for regime survival or the last chance to punish those whose actions led to the regime's collapse.

At the same time, the United States should work to make it more difficult and risky for states such as North Korea or Iran to transfer to weapons-usable nuclear material beyond their borders should they someday choose to attempt to do so. This would include working with China and other states bordering North Korea to beef up border controls and nuclear detection capabilities at key border crossings (an effort that was just beginning as of late 2006[73]), attempting similar efforts with neighbors of states such as Iran and Pakistan[74] (an even more difficult problem, given the scale of smuggling of all types of contraband that has traditionally taken place across these loosely controlled borders), and continued efforts to beef up international collaborations focused on blocking such transfers, such as the Proliferation Security Initiative (PSI). There should be no assumption, however, that such efforts to interdict transfers will decrease the probability of successful transfers by more than a few percent: blocking transfers of material that would fit in a suitcase, across hundreds or

---

[72] For discussions emphasizing this approach, see, for example, Michael Levi, "Deterring Nuclear Terrorism," *Issues in Science and Technology* 20, no. 3 (2004; available at http://www.issues.org/20.3/levi.html as of 28 December 2006); William Dunlop and Harold Smith, "Who Did It? Using International Forensics to Detect and Deter Nuclear Terrorism," *Arms Control Today* 36, no. 8 (October 2006; available at http://www.armscontrol.org/act/2006_10/CVRForensics.asp as of 28 December 2006).

[73] Interview with DOE official, December 2006.

[74] Pakistan's current government is supporting some U.S. anti-terrorist efforts, but Pakistan is clearly a plausible location from which either a future government or a terrorist group might attempt to transfer nuclear material beyond the state's borders.

thousands of kilometers of often essentially unmarked and uncontrolled borders, is an extraordinary challenge.

Countering the Nuclear Black Market

Beyond preventing nuclear theft in the first place, what can be done to reduce the chance that terrorists could acquire nuclear weapons or materials on a nuclear black market? As discussed in Chapter 3, the United States and other leading governments should take steps to make it even more difficult than it already is for potential thieves with access to nuclear material and potential terrorist buyers to find each other and complete successful transactions. Intelligence and law enforcement agencies should run additional stings and scams, posing as either buyers or sellers of nuclear material, to catch participants in this market, collect intelligence on market participants, and increase the fears of real buyers and sellers that their interlocutors may be government agents. As most of the confirmed cases in which stolen weapons-usable nuclear material was successfully seized involved one of the conspirators or some one they tried to involve in the effort informing on the others, additional measures to make such informing more likely – including anonymous tip hotlines that were well-publicized in the nuclear community, and rewards for credible information – could also have substantial benefit. All potential source states and likely transit states should have units of their national police force trained and equipped to deal with nuclear smuggling cases, and other law enforcement personnel should be trained to call in those units as needed.

Current efforts to put in place radiation detection at key border crossings (and to improve nuclear detection within the United States) may also reduce risk somewhat, forcing smugglers to pursue more difficult and chancier routes. The Domestic Nuclear Detection Office (DNDO), established after the 9/11 attacks, is focused on improving U.S. capability to detect nuclear and radiological material coming into the United States, and within the United States – as well as designing a "global detection architecture" to be implemented by other agencies. At the same time, as of late 2006 there was broad support in Congress for legislation that would require that every one of the millions of cargo containers arriving at U.S. shores each year go through a radiation scan. But as just noted, given the immense range of different methods available for smuggling items as small as the nuclear material for a bomb, it is not likely that such border-detection and internal-detection measures will reduce the probability of successful nuclear terrorism by more than a few percent.[75] To gain the maximum benefit attainable from such measures, a systems-engineering approach is needed, looking not just at how well an individual detector may perform, but what options adversaries would have to choose other routes, bribe participants to get past detectors, and take other actions to overcome the detection system – and what options the defense might have for countering those adversary tactics. Based on such an analysis, the United States and other leading governments should seek to pull existing efforts together into a prioritized strategic plan that goes well beyond detection at borders, detailing what police, border, customs, and

[75] For a discussion of measures in this area and their strengths and weaknesses, see Anthony Wier, "Interdicting Nuclear Smuggling," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/cnwm/interdicting/index.asp as of 1 March 2005).

intelligence entities in which countries should have what capabilities by when – and what resources will be used to achieve those objectives.

Global Nuclear Emergency Response

Within the United States, the Nuclear Emergency Support Team (NEST, formerly the Nuclear Emergency Search Team) is charged with searching for and disabling a terrorist nuclear bomb, in the event of a nuclear terrorist threat or other information suggesting that such an attack may be imminent.[76] NEST teams would also be called on to search for and attempt to recover nuclear material if a major nuclear theft occurred within the United States. NEST teams are equipped with sophisticated nuclear detection equipment and specialized technologies which, it is hoped, would make it possible to disable even a booby-trapped bomb before it went off. Because of the great difficulty of detecting nuclear material at long range, broad-area searches are not practicable; if the only information available was that there was a nuclear bomb somewhere in a particular city, the chances of finding it would be slim. But if additional information made it possible to narrow the search to an area of a few blocks, the chances of finding it would be substantial. The United States should work with other countries to ensure that an international rapid-response capability is put in place – including making all the necessary legal arrangements for visas and import of technologies such as the nuclear detectors used by the NEST team (some of which include radioactive materials) – so that within hours of receiving information related to stolen nuclear material or a stolen nuclear weapon anywhere in the world, a response team could be on the ground, or an aircraft with sophisticated search capabilities could be flying over the area.

Stabilizing Employment for Nuclear Personnel

With Russia's economy stabilized, nuclear workers in Russia are now paid an above-average wage, on time; the desperation of the late 1990s has largely eased. The situation at many nuclear facilities has substantially stabilized.[77] With thousands of nuclear workers soon to lose their jobs as major facilities close, however, serious proliferation risks remain. (In early 2005, for example, a group of Russian Strategic Rocket Forces officers – people who had spent their career working with nuclear weapons and presumably know a great deal about security arrangements for them – became so desperate after having been left behind with their families in a remote garrison when the missile base was closed down that they agreed to bypass the Ministry of Defense and petition the United States directly for assistance.[78]) The

---

[76] For a summary of NEST and its history, see, for example, Jeffrey T. Richelson, "Defusing Nuclear Terror," *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002; available at http://www.thebulletin.org/article.php?art_ofn=ma02richelson as of 28 December 2006), pp. 38-43.

[77] For an excellent update on the status and future of Russia's nuclear complex, see Oleg Bukharin, *Russia's Nuclear Complex: Surviving the End of the Cold War* (Princeton, N.J.: Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2004; available at http://www.ransac.org/PDFFrameset.asp?PDF=bukharinminatomsurvivalmay2004.pdf as of 8 March 2005).

[78] "US Money Lost on Way to Former Russian Army Servicemen," trans. BBC Monitoring Service, *Ekho Moskvy*, 15 February 2005; Aleksey Terekhov and Yevgeniy Latyshev, "Russian Missile Officers to Petition US for Resettlement Aid," *Novye Izvestiya*, 14 February 2005. I am grateful to Charles L. Thornton for pointing this incident and its significance out to me.

threat is not just nuclear weapons scientists who might help a foreign state develop a nuclear bomb, but nuclear workers or guards who might help thieves steal the essential ingredients of a bomb.[79] The United States should work closely with Russia and other countries to take a broader approach, using all the economic tools available, to revitalizing the economies of those nuclear cities where the major facilities are closing or shrinking and to reemploying other nuclear workers and experts who could otherwise pose a proliferation threat.[80] In Russia, such efforts should not be limited to the closed nuclear cities, but should be pursued for staff and guards at nuclear facilities at open sites as well. Individuals who have left the nuclear facilities where they once worked but may still have proliferation-sensitive knowledge – including particularly retired guards and nuclear material workers who still know the details of the security arrangements at sites with nuclear weapons or weapons-usable nuclear materials, many of whom face rather grim conditions – should also be targeted by such programs, as they have not been before. The United States should put a particular focus on working with Russia to increase the effectiveness of, and reduce the insider threats posed by, the conscript Ministry of Interior guard forces that guard most nuclear sites, ideally moving to the use only of well-trained and well-paid volunteer guards at these critical facilities (a practice Russia already follows at nuclear warhead storage sites).[81]

Reducing Stockpiles and Ending Production

In addition to securing nuclear material at sites and removing material from especially vulnerable sites, actually destroying weapons-usable nuclear material and avoiding the accumulation of ever-larger stockpiles are also potentially important tools in the theft-prevention toolbox. As noted in Chapter 3, however, a building with one ton of nuclear material poses as great a theft threat as a building with 100 tons of nuclear material, so reductions in the sheer size of nuclear stockpiles may have limited effects in reducing theft risks (however worthwhile they may be for other reasons) unless they are targeted toward achieving that purpose.

One targeted stockpile-reduction approach the United States should pursue would focus on those nuclear warheads whose features to prevent unauthorized use if they are stolen are weakest. A substantial fraction of Russia's remaining tactical nuclear warheads are believed not to have modern difficult-to-bypass electronic locks to prevent unauthorized use, and in some cases these warheads are stored at remote, difficult-to-defend storage sites.[82] The

---

[79] John V. Parachini and David E. Mosher, *Diversion of NBC Weapons Expertise from the FSU: Understanding an Evolving Problem* (Santa Monica, Cal.: RAND, 2005).

[80] See "Chapter 12, Stabilizing Employment for Nuclear Personnel," in Matthew Bunn, Anthony Wier, and John Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/cnwm.pdf as of 2 January 2007), pp. 141-146.

[81] For an alarming discussion of the weaknesses of these guard forces from an official Russian source, see Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii (Reforming MVD Troops to Guard Russian Nuclear Facilities)," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9, no. 4 (Winter 2003; available at http://www.pircenter.org/data/publications/yk4-2003.pdf as of 28 February 2005).

[82] Gunnar Arbman and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part I: Background and Policy Issues*, vol. FOI-R--1057--SE (Stockholm: Swedish Defense Research Agency, 2003); Arbman and Thornton,

United States and Russia should launch another round of reciprocal initiatives, comparable to the Presidential Nuclear Initiatives of 1991-1992, but with two critical differences: this round should be focused particularly on reducing risks of nuclear theft, and it should include some monitoring to confirm that the pledged actions are being taken. As part of such an initiative, the United States and Russia should exchange information on how many tactical nuclear warheads they have, they should discuss means to reduce this number as much as possible, and they should ensure that all of them are stored in facilities with the highest practicable levels of security. In particular, the United States and Russia should each agree to: (a) take several thousand warheads – including all of those posing the greatest risk of theft[83] – and place them in secure, centralized storage; (b) allow visits to those storage sites by the other side to confirm the presence and the security of these warheads; (c) commit that these warheads will be verifiably dismantled as soon as procedures have been agreed by both sides to do so without compromising sensitive information; and (d) commit that the nuclear materials from these warheads will similarly be placed in secure, monitored storage after dismantlement.[84]

If effective security can be provided throughout the process, it would also make sense to destroy much more of Russia's stockpiles of HEU than the 500 tons covered by the current U.S.-Russian HEU Purchase Agreement, which expires in 2013. Russia has made clear that it will not renew the existing agreement – but with both uranium and enrichment services becoming scarce and expensive, there may be substantial opportunities for Russia to profit from blending down additional HEU to LEU for use in its planned domestic reactors, or for

---

Russia's Tactical Nuclear Weapons: Part II: Technical Issues and Policy Recommendations; Anatoli Diakov, Eugene Miasnikov, and Timur Kadyshev, *Non-Strategic Nuclear Weapons: Problems of Control and Reduction* (Moscow: Center for Arms Control, Energy, and Environmental Studies, Moscow Institute of Physics and Technology, 2004; available at http://www.armscontrol.ru/pubs/en/NSNW_en_v1b.pdf as of 17 March 2005).

[83] Ultimately all nuclear warheads not equipped with modern electronic locks should be dismantled. In the near term, however, neither side is likely to be willing to dismantle all such warheads, as U.S. strategic ballistic missile warheads, the centerpiece of the U.S. deterrent, are not equipped with such locks integral to the warheads, and the same is believed to be true of some warheads critical to the Russian deterrent. In general, however, warheads on submarines or on ICBMs in concrete silos pose a lesser risk of theft than warheads scattered in forward-deployed storage facilities. In particular, while these warheads may not have electronic locks requiring insertion of a particular code to arm them, they are typically equipped with devices that will not allow them to be armed until they have experienced the expected acceleration of ballistic missile flight followed by a period of coasting through space; while these devices were designed for safety, not security, they would make it quite difficult for a terrorist group not aided by someone familiar with their details to set off a stolen weapon, as discussed in Chapter 2. Hence, for the immediate initiative, for all warheads not equipped with modern electronic locks, each side should either (a) include them in the set subject to secure, monitored storage and eventual verified dismantlement, or (b) provide the other side with sufficient information to build confidence that they are highly secure. Where warheads not equipped with modern electronic locks are not in immediate use, and are not mounted on SLBMs or ICBMs – as when they are being kept as spares, for example – they should be stored in partly disassembled form, ideally with critical parts in separate locations, to make them more difficult to steal.

[84] For an earlier description of this idea, see, for example, Bunn, Wier, and Holdren, *Controlling Nuclear Warheads and Materials*, pp. 132-134. For an up-to-date discussion of the risks posed by tactical nuclear weapons and steps to reduce them, see William Potter and Nikolai Sokov, "Practical Measures to Reduce the Risks Presented by Non-Strategic Nuclear Weapons," paper presented at The Weapons of Mass Destruction Commission, Stockholm2005 (available at http://www.wmdcommission.org/files/No8.pdf as of 18 April 2005).

sales on international markets. There are also opportunities for the United States and other countries to offer increased access to their uranium and enrichment markets and other tools – including, for example, providing some of their comparatively rich depleted uranium "tails" for use in producing blendstock for blending down HEU – to encourage Russia to destroy hundreds of tons of additional HEU. There may also be opportunities, through relatively modest capital investments in expanding capacity, to accelerate the rate of blending beyond the current 30 tons of HEU per year, so that the security benefit of destroying additional HEU does not have to wait until well beyond 2013 to be achieved. The United States, for example, could pay Russia a fee for service for blending HEU to 19% enriched LEU, which would be placed in monitored storage until it could be blended to commercial levels and sold without unduly interfering with commercial markets.[85]

At the same time, if high standards of security are maintained throughout, it would be worthwhile to move forward as quickly as possible with safe, secure, and transparent disposition of excess weapons plutonium. Disposition of the 34 tons of Russian excess plutonium and the 34 tons of U.S. excess plutonium covered by the U.S.-Russian Plutonium Management and Disposition Agreement will only be a substantial contribution to U.S. and international security, however, if it is but the first step toward a much larger reduction in the stockpiles of weapons plutonium that now exist.[86]

Efforts to end the accumulation of stockpiles of weapons-usable nuclear material should also be pursued, particularly if they have ancillary benefits for reducing the dangers of nuclear theft and terrorism. If a verified and global fissile material cutoff treaty (FMCT) could be achieved, for example, this would not only end further additions to the stockpiles of plutonium and HEU available for weapons, but would likely bring to an end a substantial amount of bulk processing of plutonium and HEU (one of the stages of the material life-cycle that is most vulnerable to insider theft), and the verification would impose a multilateral discipline on the quality of material control and accounting that is not present at military facilities in the nuclear weapon states today.[87] The United States should reverse its misguided opposition to a verified fissile cutoff, and the United States and other leading governments should seek to overcome the obstacles to negotiating such a treaty – including the possibility

---

[85] The Nuclear Threat Initiative has been sponsoring detailed studies of such accelerated blend-down options by experts from the Russian facilities doing the blending work. See Laura Holgate, "Accelerating the Blend-Down of Russian Highly Enriched Uranium," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005; available at http://www.nti.org/c_press/analysis_Holgate_INMM%20Paper_061005.pdf as of 28 December 2006). For an earlier description of such proposals, see Bunn, Wier, and Holdren, *Controlling Nuclear Warheads and Materials*.

[86] For an elaboration of this point, see Matthew Bunn, testimony in Subcommittee on Strategic Forces, Committee on Armed Services, *Plutonium Disposition and the U.S. Mixed Oxide Fuel Facility*, U.S. House of Representatives, 109th Congress, 2nd Session, 26 July 2006 (available at http://www.house.gov/hasc/schedules/ as of 10 August 2006).

[87] I am grateful to William Walker for making this point to me. Personal communication, March 2003.

of undertaking negotiations outside of the Conference on Disarmament if that body continues to be unable to move forward.[88]

The United States and other countries are also working with Russia to provide alternative heat and power sources so that Russia's last plutonium production reactors can shut down. Like the FMCT, this would also lead to the end of a large quantity of bulk processing of plutonium and HEU each year (both at the reprocessing plants that recover the plutonium produced in these reactors and at the facilities that produced HEU spike fuel for these reactors – which is also transported over thousands of kilometers from the fabrication facilities). These reductions in bulk processing would reduce the danger of nuclear theft from these facilities. At the same time, though, the impending closure of these facilities means that thousands of workers who have access to plutonium today know that they will soon be losing their jobs, which may increase temptations for nuclear theft. If this effort is to have net security benefits worth its very substantial costs, the participating countries should put high priority on working with Russia to ensure that the displaced workers receive either suitable employment or secure retirement packages and that high levels of security – including against insider threats – are maintained throughout these facilities' remaining life.

Modified Approaches to Increase the Chances of Success

The steps outlined above represent a broad and ambitious agenda. That agenda can only succeed if countries throughout the world actively cooperate toward these ends. Six key changes in past U.S. approaches are likely to be needed to gain that cooperation and overcome the obstacles to progress:

- new steps to build the sense of urgency about, and commitment to addressing, the threat of nuclear terrorism among political and nuclear leaders around the world;
- sustained leadership from the highest levels (including the appointment, in the United States and Russia, and possibly in other participating countries as well, of senior officials with direct access to the head of state when needed, with full-time responsibility for leading the myriad efforts directed toward preventing nuclear terrorism);
- development of an integrated and prioritized plan, tying together the many policy tools focused on reducing the dangers of nuclear theft and terrorism;
- truly partnership-based approaches, incorporating ideas and resources from all cooperating partners, moving away from donor-recipient relationships;
- more flexible approaches to nuclear security cooperation that can allow important improvements to be made without in all cases requiring that U.S. personnel be able to travel to the most sensitive nuclear sites; and

---

[88] Matthew Bunn, "Fissile Material Cutoff Treaty," in *Nuclear Threat Initiative Research Library: Securing the Bomb*, ed. Matthew Bunn and Anthony Wier (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/ending/fmct.asp as of 2 January 2007).

- expanded efforts to ensure that high levels of nuclear security will be sustained for the long haul and to build strong "security cultures," in which all staff relevant to security give it the priority it deserves.

Approach 1: Strengthening the Sense of Urgency and Commitment

The single most essential ingredient of success in ensuring security for nuclear stockpiles around the world is convincing political leaders and nuclear managers around the world that the threat of nuclear terrorism is real and that improvements in nuclear security are critical to their own national security and deserving of their own resources. If the leaders of all the key states and nuclear facilities around the world were convinced of those two points, they would be likely to take the actions needed to keep these stockpiles out of terrorist hands. But if they are not convinced – as many of them are not today – there is little chance that they will assign sufficient resources, impose stringent security rules, take political risks to allow sensitive nuclear cooperation with foreigners, or take the other actions needed to achieve and sustain security levels sufficient to defend nuclear stockpiles against demonstrated terrorist and criminal threats. In maintaining a strong safety system, it is sometimes said that the most important element is "forgetting to be afraid."[89] The same is even more true for nuclear security.

But today, many of the key players are not afraid. They believe, with Pakistani President Musharraf, that the United States is "overly concerned" about the possibility of nuclear terrorism. The common attitude was well summed up in a private interview with a a leading Russian nuclear expert – who had played a key role in establishing cooperation to improve security in the 1990s. Asked about the threat of nuclear theft in Russia today, he leaned back in his chair, took a drag on his cigarette, and said: "I am not worried."[90] Several key steps should be taken to try to build the sense of urgency and commitment among political leaders, nuclear managers, and all key personnel involved in nuclear security.

Joint threat briefings. A series of briefings for political leaders of particular countries participating in the global coalition (and their U.S. counterparts, for political symmetry), given jointly by nuclear experts from the United States and each of the countries where the briefings took place, could outline in detail the terrorist desire for nuclear weapons, their proven efforts to get nuclear weapons, and the very real possibility that terrorists could make at least a crude nuclear bomb if they got the needed nuclear materials. The briefings could also highlight the likely global economic and political effects if a terrorist bomb were to be detonated in a major city, along with the significant reductions in this risk that could be achieved through improved nuclear security measures and other steps.

Fast-paced national surveys of nuclear security vulnerabilities. In the aftermath of the 9/11 attacks, DOE dispatched a team of security experts to urgently review security measures at all key DOE nuclear sites and make recommendations for improvement. As noted in Chapter 1, a similar approach of sending out a trusted team for an urgent review had

---

[89] James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, U.K.: Ashgate, 1997), p. 195.
[90] Interview with Kurchatov Institute official, September 2003.

been undertaken several times in the past as well. These reviews have typically identified a wide range of vulnerabilities requiring correction.

President Bush should seek to convince the leaders of key states with nuclear stockpiles to pick teams of security experts they trust to conduct fast-paced assessments of potential vulnerabilities and to develop recommendations for fixing them at all sites with nuclear weapons or weapons-usable nuclear material in their countries. These reviews could ask whether the security measures in place are really good enough to defeat, for example, one to three well-placed insiders conspiring to steal nuclear material, or two teams of well-armed and well-trained outside attackers attempting to break in, who might have help from one or more insiders. In many countries, any thorough review would conclude that for some facilities, the answer is decidedly "no." Such reviews could give these leaders an unvarnished, independent assessment, going around those with an incentive to tell them that everything is secure. No U.S. personnel need take part, so there need be no revelation to the United States or other foreigners of any specific security vulnerabilities. But the United States should share, in general terms, the experiences it has had in performing such rapid initial assessments, it should provide training in vulnerability assessment and testing techniques, and, in those countries where assistance may be needed, it should offer to help cover the cost of any security upgrades the reviews recommend.

Realistic security performance tests. A regular system of realistic testing of security performance, where "red teams" playing the roles of outside attackers or insider thieves attempt to overcome the system, can be a critical part of convincing non-expert political leaders that more resources are needed for security. Short of real thefts, nothing demonstrates more convincingly that there is a problem than spectacular failures of defense systems to protect nuclear items in realistic tests. Moreover, if done properly, such tests can help convince guards and other security personnel of the plausibility of the threat, provide important training, and help them find and fix problems that may not have been obvious in paper studies. Such performance testing has been a critical part of improved nuclear security over the past two decades in the United States.[91]

The United States should work with key countries participating in the global coalition to convince them to institute regular realistic testing of nuclear security, briefing them on the U.S. experience, providing training in testing techniques, and offering to cover part of the cost of conducting such tests. In cases like Russia's where cooperation with U.S. experts is particularly extensive, the United States should seek to help establish joint security testing teams, which could train together, share their techniques, and perhaps carry out joint tests at a few non-sensitive facilities. This would provide both the United States and Russia with a greatly increased understanding of the other side's approach to testing security.

Nuclear terrorism wargames. Wargames and similar exercises have been effective in getting policymakers in a number of countries to understand at intellectual, emotional, experiential levels the urgent challenges they face. A wargame or series of wargames for

[91] For a good account of part of this experience, see Oleg Bukharin, "Physical Protection Performance Testing: Assessing U.S. NRC Experience," *Journal of Nuclear Materials Management* 28, no. 4 (Summer 2000).

Russia's national security policymakers, focused on nuclear theft and terrorism (similar to an exercise recently conducted in Europe) could help convince participants that more needs to be done to secure nuclear stockpiles.[92]

Shared threat incident databases. Most nuclear managers and staff – even those whose jobs are critical to security – do not receive regular information about terrorist attempts to acquire nuclear materials or nuclear weapons, or other security incidents from which lessons can and should be drawn about the kinds of threats nuclear facilities must be defended against. In 2003, for example, a Russian court case revealed that a Russian businessman had been offering $750,000 for stolen weapon-grade plutonium for sale to a foreign client and had made contact with residents of the closed nuclear city of Sarov in an attempt to get such material.[93] While he did not succeed, the fact that a Russian was offering what was then roughly a century of the average nuclear worker's salary for such material is surely a relevant fact of which security managers should be aware. No Russian nuclear expert or security manager with whom I have discussed this case had ever heard of it before.[94] Similarly, most nuclear security managers around the world would probably be amazed to hear that there really has been a case in the past of more than a dozen heavily armed terrorists overpowering the armed guards at a nuclear facility and seizing complete control of the facility – a type of threat that is sometimes dismissed as unrealistic.[95]

In organizational systems for safety (as opposed to security), keeping track of all such incidents and "near-misses" and the lessons learned from them has proved to be absolutely critical. It is a key part of convincing staff of the need to take safety seriously. Indeed, extensive studies have concluded that "the two characteristics most likely to distinguish safe organizations from less safe ones are, firstly, top-level commitment and, secondly, the possession of an adequate safety information system."[96] In the United States, the Institute for Nuclear Power Operations (INPO, the U.S. arm of WANO) distributes detailed analyses of all safety-related incidents to all plants, with accompanying "lessons learned" to avoid such

---

[92] The Center for Strategic and International Studies and the Nuclear Threat Initiative (NTI) organized the "Black Dawn" war game in Europe and are undertaking a similar effort in Moscow. These are very promising first steps; more such games should be conducted, for key officials and facility managers in countries around the world.

[93] Matthew Bunn, "Anecdotes of Insecurity," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/threat/anecdote.asp as of 2 January 2007).

[94] Interviews, May, July, and October 2005.

[95] This was at the Atucha Atomic Power Station in Argentina in 1973. The facility was under construction at the time and had no nuclear material on-site. The terrorists departed as a response force arrived, after a brief shoot-out with the responders. Konrad Kellen, "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists," in *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Cambridge, Mass.: Lexington Books for the Nuclear Control Institute, 1987).

[96] Reason, *Managing the Risks of Organizational Accidents*, p. 113.

problems in the future. It later inspects each plant's program for reviewing these incidents and implementing the lessons learned.[97]

Although security matters face the constraints of secrecy, in many cases a similar approach can and should be taken for nuclear security. The United States should work with its international partners to establish a shared database of verified information on important security-related incidents and related lessons for the future. Rules could then be put in place requiring facilities to review these incidents and implement the applicable lessons. The incidents included should go beyond the nuclear industry itself. Incidents that confirm the ways that terrorists and thieves have used tactics such as bribing or blackmailing insiders (for example by kidnapping their families), deception (such as fake uniforms and IDs), unusual vehicles, tunnels into secure vaults, and attacks with substantial force and heavy armament would be important for nuclear security managers around the world to understand.[98] Many of these specifics of past incidents are not classified and could be included in a database that was available to nuclear facilities around the world. Creating such a threat incident database and ensuring that it was regularly updated and widely used could do a great deal to increase security awareness and strengthen security culture. Such a threat incident database, like many of the other commitment-building steps suggested here, could potentially be implemented by an industry-led security initiative such as the proposed WINS.

A description of the 1992 theft of 1.5 kilograms of 90% enriched HEU from the Luch Production Association in Podolsk, Russia, for example, might note that the thief stole the material in small quantities at a time, to avoid detection by the crude accounting system in place at the time at the facility; that the facility had no portal monitors in place at the time to detect HEU being carried out the door; and that the thief was motivated by fear that the hyperinflation in Russia at the time would make him unable to provide for his family.[99] There are several lessons to be learned from just this one case. Facilities should first of all ensure that effective portal monitors are in place to detect any removal and that there are no means of getting material out of a facility without going through a portal monitor (such as passing it out a window). To prevent thefts like this example, facilities should ensure that portal monitors provide their data not only to a guard by the portal monitor (who might be bribed or threatened to ignore a signal), but also to a remote location. Facilities should put in place accounting systems capable of detecting significant removals of nuclear material, or at least measures to compensate if the accounting system was not sensitive enough to do that job in a timely way. Finally, facilities would be wise to monitor the financial status of employees with access to nuclear material, perhaps removing from access to nuclear material employees identified as financially desperate.

Threat-focused training. Ongoing training for nuclear security personnel should highlight the urgency of maintaining high security, ideally in graphic terms that get to the

---

[97] Rees, *Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island*, pp. 128-150.
[98] See Chapter 4 for a discussion of a selection of incidents involving such tactics.
[99] For an interview with the thief describing the crime, see "Frontline: Loose Nukes: Interviews" (Public Broadcasting System, 1996; available at http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/ as of 22 December 2005).

heart, as well as the head. As a related example, as part of the safety training program for all of those involved in building and maintaining U.S. nuclear submarines so that they will not leak, key personnel are required every year to listen to a several-minute audiotape of a submarine that failed, killing everyone aboard.[100] Presentations to policymakers and key nuclear security officials of images from Hiroshima and Chernobyl might similarly highlight, in an emotionally gripping way, the scale of the catastrophe that could occur if nuclear security measures failed and terrorists succeeded in detonating a nuclear bomb or sabotaging a major nuclear facility. The United States and Russia should work together, for example, to develop a training video for nuclear personnel highlighting terrorists' ongoing hunt for nuclear material for nuclear weapons and the possibility that particularly sophisticated terrorist groups might be capable of constructing at least a crude nuclear bomb.

Approach 2: Sustained High-Level Leadership

A second essential approach is sustained leadership from the highest levels of government, focused on overcoming obstacles and moving these programs forward as rapidly as possible. The job of keeping nuclear weapons and their essential ingredients out of terrorist hands requires broad international cooperation affecting some of the most sensitive secrets held by countries around the globe. A maze of political and bureaucratic obstacles must be overcome – quickly – if the world's most vulnerable nuclear stockpiles are to be secured before terrorists and thieves get to them.

The U.S.-Russian interagency nuclear security committee established by the Bratislava summit, co-chaired by Secretary of Energy Samuel Bodman and his Russian counterpart, Rosatom chief Sergei Kirienko, represents a major step in the right direction. This committee has succeeded in reaching agreement on a plan for completing upgrades at all but a few Russian nuclear weapon and weapons-usable material sites by the end of 2008 and a plan for returning most Soviet-origin HEU to Russia by the end of 2010. Those agreed timetables, coupled with a requirement to report to President Bush and President Putin every six months on progress in meeting them, have focused managers' minds on moving these efforts forward as quickly as they possibly can; indeed, DOE managers acknowledge "raiding" funds from efforts not covered by the Bratislava mandates in order to find enough money to meet the agreed Bratislava deadlines.[101] In other words, post-summit process is having precisely the desired effect: forcing managers to do everything they can to move the targeted efforts forward. The twice-yearly reports to the U.S. and Russian Presidents also provide a regular mechanism that could be used to bring key issues forward for presidential decision (though it does not appear to have been used for that purpose to date).

But the reality is that the necessary programs stretch across multiple branches of government – in the United States, in Russia, and in other essential participants in the global coalition described above. Many of the obstacles are not ones that a secretary of energy or a

---

[100] See testimony of Rear Admiral Paul E. Sullivan, Naval Sea Systems Command, in Committee on Science, *NASA's Organizational and Management Challenge*, U.S. Congress, House of Representatives, 29 October 2003.

[101] Interview with DOE officials, October 2006.

Rosatom chief can realistically overcome; for better or for worse, neither of these agencies are at the center of decision-making on matters of security, diplomacy, or secrecy and counter-intelligence in their respective governments. Agencies such as these must inevitably take the lead on implementation, but they need sustained help from the centers of political power in overcoming the obstacles to implementation and seizing new opportunities as they arise.

To ensure that this work gets the priority it deserves, President Bush should appoint a senior full-time White House official, with the access needed to walk in and ask for presidential action when needed, to lead these efforts and keep them on the front burner at the White House every day. That official would be responsible for finding and fixing the obstacles to progress in the scores of existing U.S. programs scattered across several cabinet departments of the U.S. government that are focused on pieces of the job of keeping nuclear weapons out of terrorist hands – and for setting priorities, eliminating overlaps, and seizing opportunities for synergy. Despite the creation of a Department of Homeland Security, President Bush rightly considered it essential to continue to have a senior official in the White House focused full-time on homeland security – to ensure that the issue continued to get the needed sustained White House attention and to use the power of the White House to overcome the obstacles to progress and cut through the disputes between the many departments and agencies that continue to play essential roles. Much the same logic applies in this case.

The fate of the Mayak Fissile Material Storage Facility (FMSF) provides one graphic example of the need for such a mechanism for sweeping aside bureaucratic obstacles. The FMSF is a giant secure fortress for storing excess plutonium, built in Russia with over $300 million in U.S. funds, and was completed in 2003. But because of a variety of disputes over transparency, adequate staffing, and other issues, it sat empty for three long years, with the first plutonium loaded in the summer of 2006 (with the transparency issues still not resolved).[102] These were three years that were taking place after the 9/11 attacks and after Russian officials had acknowledged that terrorist teams were scoping nuclear weapon storage facilities in Russia; half of the time was after the Bratislava summit had focused presidential attention on accelerating progress on nuclear security. Faster mechanisms for overcoming obstacles and escalating disputes to higher levels when necessary are urgently needed.

As part of this sustained leadership from the top, nuclear security needs to be moved much closer to the front of the diplomatic agenda. Despite myriad statements about the priority of the issue, there is little public indication that the subject of preventing nuclear terrorism – and in particular urgent steps to secure nuclear stockpiles around the world – has been a focus of any but two of President Bush's meetings with foreign leaders, or of Secretary

---

[102] For an announcement of the initial loading of plutonium in July 2006, see "Nuclear Storage Facility Commissioned in Russia's Chelyabinsk Region," *ITAR-TASS*, 11 July 2006. For accounts of some of the disputes about the facility, see Matthew Bunn, "Mayak Fissile Material Storage Facility," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/securing/mayak.asp as of 2 January 2007); Carla Anne Robbins and Anne Cullison, "Closed Doors: In Russia, Securing Its Nuclear Arsenal Is an Uphill Battle," *The Wall Street Journal*, 26 September 2005.

of State Condoleezza Rice's meetings with any of her counterparts. The subject was entirely absent from the U.S.-India nuclear deal, despite the fact that DOE experts had been attempting to engage India on nuclear security cooperation for years. No public discussion of Chinese leader Hu Jintao's April 2006 visit to Washington mentioned the subject, even though DOE has placed high priority on trying to extend nuclear security cooperation with China, but has not yet succeeded in getting Chinese agreement to expand beyond the civil sector.

If an effective global coalition to prevent nuclear terrorism is to be forged, this has to change. The leaders of the critical states need to hear, at every opportunity, that action to ensure nuclear security is crucial to their own security and to a positive relationship with the United States. The United States can no longer afford to let the issue languish when obstacles are encountered, or to leave the discussion to specialists. The United States government should make nuclear security a central item on the diplomatic agenda with all of the most relevant states, an item to be addressed at every opportunity, at every level, until the job is done.[103]

Approach 3: An Integrated, Prioritized Plan of Action

Literally dozens of different programs in several different agencies of the U.S. government are addressing one aspect or another of reducing the threat of nuclear terrorism. Yet today, there is no integrated plan linking these efforts together, no systematic means of identifying opportunities for synergy or gaps or overlaps to be corrected, and little effort to prioritize which of these efforts are most important. When Congress passed legislation requiring the administration to prepare a prioritized plan for securing the world's most dangerous facilities, what they got were three prioritized lists from three of DOE's programs – even within DOE, the programs were not able to negotiate out a consolidated set of priorities, let alone doing so between DOE and other agencies.[104]

---

[103] The experience in Russia has been that cooperation has proceeded best when either (a) it was allowed to go forward "under the radar screen," with technical experts communicating directly with each other with relatively modest intervention from central governments, or (b) at the other extreme, when action was taken at the presidential level to push the cooperation forward and overcome obstacles. When the discussion was lodged at levels in between those extremes, officials who wanted to raise objections were able to do so, and officials who wanted to sweep aside these obstacles did not have the power to do so. Matthew Bunn, "Cooperation to Secure Nuclear Stockpiles: A Case of Constrained Innovation," *Innovations* 1, no. 1 (2006; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/INNOV0101_CooperationtoSecureNuclearStockpiles.pdf as of 4 April 2006). In the case of countries such as Pakistan, India, and China, however, it appears likely that nuclear security cooperation will be so sensitive and so closely monitored by conservative government security agencies, that the "under the radar screen" approach may not be possible.

[104] The unclassified version of this "plan" has almost no content, but does acknowledge that the classified version includes three separate lists of the highest priorities for three different programs, based on each program's own separate methodology for assessing priorities. U.S. Department of Energy, National Nuclear Security Administration, *Report to the United States Congress under Section 3132 of the FY 2005 Defense Authorization Act: Unclassified Executive Summary* (Washington, D.C.: DOE, 2006). That this was because the different programs each had their own priorities and did not come to any agreement on overall priorities is from an interview with a DOE official, November 2005.

One of the first jobs of a senior White House official to lead these disparate efforts must be to establish priorities and put together a plan that includes objectives to be achieved, assignment of responsibility for different aspects of achieving them, milestones for progress, and the resources needed to get these jobs done. That official must then hold managers accountable for making the progress needed and quickly identifying obstacles to progress and possible ways to resolve them along with opportunities for new progress and ways to take advantage of them. Of course, circumstances change – some tasks turn out to be more difficult than expected and new opportunities arise. Hence the plan must be regularly updated and modified. The President and Congress should act to ensure that sufficient resources are assigned so that lack of money or personnel is never a substantial constraint on efforts that could substantially reduce the risk of nuclear terrorism.

Approach 4: Building Genuine Nuclear Security Partnerships

Gaining both the in-depth cooperation required to improve security for all the vulnerable nuclear stockpiles around the world and the buy-in of national experts crucial to long-term sustainability will require approaches based on genuine partnership. Experts from the countries where these stockpiles are located will need to play key roles in working with foreign partners in the design, implementation, and evaluation of the entire effort.[105] Indeed, data from a wide range of other types of international assistance efforts makes clear that the success rate is far higher when assistance recipients are deeply involved in project design and implementation than when this is not the case.[106] Moreover, whatever transparency a country is willing to provide about the size and management of its nuclear stockpiles, that country's experts will inevitably know more about those stockpiles, the specific approaches used to secure them, their security, and the agencies charged with ensuring that security than American experts ever will.

As noted earlier, for proud and secretive countries such as China, India, and Pakistan, nuclear security cooperation that is portrayed as an opportunity for them to join in a co-equal partnership with the leading nuclear states to address a global security problem will be far more appealing than being seen as needing foreign assistance because they are too poor or uninformed to adequately secure their own nuclear stockpiles. The specific tactics and sets of incentives needed to move cooperation forward will vary with national and cultural contexts. But in broad terms, approaches based on genuine partnership will work better than attempting to impose "made in America" nuclear security approaches.

How would a real, and not just rhetorical, shift from assistance to partnership actually be different from the approaches that have been taken in the past? In the case of cooperation in Russia, there has already been a significant and positive shift in recent years. Russian

---

[105] For discussions of such partnership approaches to nuclear security in the Russian context, see Oleg Bukharin, Matthew Bunn, and Kenneth N. Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union* (Washington, D.C.: Russian American Nuclear Security Advisory Council, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mpca2000.pdf as of 2 January 2007); Bunn, "Building a Genuine U.S.-Russian Partnership for Nuclear Security."

[106] See, for instance, World Bank, *Assessing Aid: What Works, What Doesn't, and Why* (Oxford, United Kingdom: Oxford University Press, 1998).

experts are now responsible for designing, installing, and maintaining the upgraded nuclear security and accounting systems (with substantial oversight from U.S. experts where the United States is providing the funds). Since Bratislava, the two sides have begun a more open discussion of both "best practices" in nuclear security and difficulties they have encountered in providing security for their nuclear stockpiles. But there are still shifts to be made to make this effort a genuine partnership. Russia would have to assign more of its own resources to the effort, reversing the past habit, in many areas, of cutting Russian funding for activities the United States is willing to help pay for. It would also need to be willing to openly discuss key issues for the joint effort, such as how nuclear security arrangements are and will be funded, or how good security performance by managers, guards, and workers is and will be rewarded. The United States would have to be willing to bring Russian experts more fully into the process by which decisions are made on what security upgrades will be done with U.S. funds.

Strategic plans, timetables, and milestones should be developed jointly by the country where the nuclear stockpiles in question exist and its foreign partners, using both the country's own funds and foreign funds. They should not be developed in Washington alone, without consulting with the agencies which actually control those stockpiles, as has sometimes been the practice in the past. Similarly, guidelines for the kinds of upgrades to be put in place and the standards of security needed should be discussed and agreed wherever possible. In the past, the United States has often decided what kinds of security measures to tell its teams to put in place in Russia without consulting Russian experts – keeping those experts from seeing those guidelines even as they were used as the basis to reject security upgrade projects that Russian experts proposed. Progress should be reviewed by experts from both sides working together, replacing the past U.S. practice of having U.S.-only evaluation teams assess progress of each project and recommend changes. Key personnel should lead the effort at particular sites for extended periods of time, so they can build the site-level relationships needed for a real partnership to grow.

A partnership approach does not necessarily mean putting U.S.-funded projects under management from the country where the nuclear stockpiles are located – an arrangement that might well slow projects down rather than speeding them up. A good example of how the kind of partnership recommended here works in practice can be found in the case of the work to improve security and accounting for the nuclear warheads and materials of the Russian Navy. In that case, a small, stable U.S. team has been leading the effort for years, building confidence with Russian counterparts over time. A Russian team at the Kurchatov Institute has taken the lead in overseeing much of the work. With a daily on-the-ground presence in Moscow and Russian security clearances, the Kurchatov team has been able to overcome obstacles far more effectively than remote U.S. managers would have been able to do. Finally, a highly committed Russian Navy team has been willing to make the hard decisions needed to move forward and has provided Navy resources for sustaining the new security and accounting equipment once installed.[107]

---

[107] For an account, see, for example, Morton Bremer Maerli, "U.S.-Russian Naval Security Upgrades: Lessons Learned and the Way Ahead," *Naval War College Review* 56, no. 4 (Autumn 2003; available at http://www.nwc.navy.mil/press/Review/2003/Autumn/pdfs/art2-a03.pdf as of 18 April 2005).

With the world's largest nuclear stockpiles, a growing cadre of specialists with experience in modern security and accounting techniques, and political relationships with a range of countries unlikely to be willing to cooperate with experts from the United States, Russia is in an excellent position to make a major contribution to a global coalition. The United States should encourage Russia to take a leadership role in the new Global Initiative Russia co-founded, offering technical assistance in nuclear security and accounting to countries around the world. Even at U.S. facilities, as part of the ongoing discussion of "best practices," when Russian experts visit, the United States should actively solicit their suggestions for security improvements and should make a conscious effort to adopt in the United States any Russian equipment, software, or procedures that may be useful. Few steps could more quickly dispel the perception of Russia as a passive recipient of U.S. assistance than well-publicized U.S. adoption of an innovative piece of Russian equipment or a Russian procedure superior to U.S. approaches for improving security at U.S. nuclear facilities.

Such genuine partnerships cannot be built in a political vacuum. Today, while President Bush and President Putin have a good relationship, much of the Russian security establishment is deeply suspicious of cooperation with the United States – and much of the U.S. political establishment is becoming more and more suspicious of cooperation with a Russia seen as sliding back toward authoritarianism and seeking to dominate its neighbors.[108] Similarly, many in the U.S. and Chinese nuclear establishments are deeply suspicious of the other side, with each country seeing the other as bent on stealing nuclear secrets. Much the same is true of India and Pakistan – though the specifics of the suspicions vary in each case. A key focus of the top-level leadership needed to secure the world's nuclear stockpiles must be to find the means to overcome these suspicious and build the partnerships needed to move forward.

In many cases, a willingness to cooperate in other areas important to partner countries will be one key to building an effective partnership. Though nuclear security was left out of the U.S.-India agreement, the U.S. willingness to lift nuclear sanctions on India undoubtedly increases the chances that nuclear security cooperation with India will finally move forward. The recent U.S. decisions to invite Russia to join in the Generation IV International Forum, to ask Russia to join in the Global Nuclear Energy Partnership (GNEP), and to negotiate a peaceful nuclear cooperation agreement with Russia (a so-called 123 agreement, after the relevant section of the Atomic Energy Act) are steps in the right direction – though the United States and Russia will have to be careful to ensure that such cooperation does not lead to promoting fuel cycle strategies that increase proliferation risks rather than decreasing them.[109]

Overcoming the suspicions and political tensions standing in the way of effective nuclear security partnerships with all the critical states will require a sustained diplomatic effort. Doing so is nonetheless an essential ingredient of success in reducing the threats of

---

[108] John Edwards and Jack Kemp, with Stephen Sestanovich, *Russia's Wrong Direction: What the United States Can and Should Do*, ed. Stephen Sestanovich, Independent Task Force Report No. 57 (New York: Council on Foreign Relations, 2006; available at http://www.cfr.org/content/publications/attachments/Russia_TaskForce.pdf as of 17 May 2006).

[109] For a discussion of these dangers, see testimony of Matthew Bunn in *Global Nuclear Energy Partnership.*

nuclear terrorism. As part of that effort, the United States should undertake a substantially increased public diplomacy effort to build support for cooperation to secure, consolidate, and eliminate nuclear stockpiles, in Russia and around the world. The United States should sponsor articles, workshops, briefings, equipment displays, and related events and publications that emphasize such matters as how much has been accomplished that serves the security interests of Russia and the other states where this cooperation is taking place; how limited the access to sensitive sites the United States has requested really is and how few nuclear secrets are actually revealed; how willing the United States has been to give parallel access at its own sites; how large the fraction of the equipment that is being installed that is produced by local manufacturers, in systems designed and installed by local experts, not American ones; and how beneficial to the local public's safety and security this cooperation has been. Expanded efforts should be pursued to build support through engaging the legislatures, the press, non-government organizations, and the rest of civil society in the countries where such cooperation is taking place.

Approach 5: Cooperating Without Compromising Nuclear Secrets

Disputes over access to sensitive sites and protection of nuclear secrets have delayed a wide range of cooperative nuclear security upgrade efforts, in Russia and elsewhere – sometimes for years at a time. To ensure that taxpayers' funds are spent appropriately, the United States has often demanded that U.S. personnel be allowed access to the sites where U.S. money was to be spent on security upgrades. But some sites in Russia have simply been too sensitive for Russia to allow foreigners to visit – and this is likely to be even more true in countries such as Pakistan, India, and China, where the very existence of some of the important sites (such as warhead storage sites) are closely guarded secrets.

The United States and other donor countries should take a flexible approach to these issues, working creatively to find ways to cooperate to improve nuclear security within the constraints of what partner states are willing to accept. In the end, it is more important to make progress in ensuring that nuclear stockpiles are secure than it is to keep track of every dollar of U.S. funds.

Approaches developed in the course of U.S.-Russian cooperation can be used in some cases. For example, in a number of cases, the U.S. government has taken the view that if it was only providing equipment to be installed by the partner country at its own expense, U.S. personnel did not need to visit, or even know the location of, the places where the equipment was installed. For particularly sensitive sites, U.S. and Russian laboratory experts worked out approaches that can provide good assurance that U.S. funds are spent appropriately without access by U.S. personnel, such as photographs and videotapes of installed equipment, certification of installation by facility directors, and operational reports on the equipment's use. Another innovative approach that has been implemented in some cases is reliance on "trusted agents" – personnel who are citizens of the recipient country with security clearances from that country, who can visit relevant sites and certify that work has been done appropriately, but who are employed by a U.S. contractor.

There are a wide variety of other steps that can be taken cooperatively to improve nuclear security without compromising nuclear secrets. These include: training experts in vulnerability assessment, physical protection system design, material accounting, nuclear security regulation, and other areas of expertise critical to an effective nuclear security and accounting system; discussions of "best practices" and means to find and fix nuclear security vulnerabilities; and joint exercises and demonstrations of equipment and procedures, carried out at non-sensitive facilities.

Approach 6: Ensuring Sustainability and Strong Security Cultures

As noted above, as U.S.-Russian cooperative security upgrade programs race toward a 2008 deadline for completing upgrades, the questions of how to ensure "sustainability" and strong "security cultures" are among the most difficult remaining policy challenges facing these efforts – not only in Russia, but everywhere where cooperation to improve nuclear security will proceed around the world. Sustaining for the long haul the enhancements to security made possible by one-time international investments in security systems will require countries to indigenously finance, manage, and maintain their own security systems. Therefore, working with partner countries to ensure that high levels of security will be sustained for the long haul and that all personnel give security the priority it deserves are absolutely essential if the risk of nuclear terrorism is going to be substantially reduced for an extended period.[110]

These are genuine concerns. Achieving sustainability will require a much higher commitment to modern security and accounting measures, and far more resources for them, than has been forthcoming from the Russian government or Russian facility managers to date. Similar issues are certain to arise elsewhere as well. While many types of equipment are being installed in cooperative nuclear security programs, substantial portions of the equipment have expected lifetimes averaging around 5-15 years – meaning that some 10% of it might have to be replaced in an average year. In Russia alone, the average annual cost of these replacements – to say nothing of routine operations and maintenance, salaries and other costs for guards and other security and accounting personnel, and other security costs – is likely to come to over $100 million per year (if one considers both the equipment for nuclear material sites and the equipment for nuclear warhead sites). The current sums allocated for nuclear security and accounting equipment by the Russian government and by individual facilities are not publicly known, but are clearly far below this figure. (As noted in Chapter 2, one leading Russian expert estimated in 2005 that spending on physical protection comes to only 30% of the need.) And resources are not the only issue: sustaining high levels of nuclear security requires a high level of commitment to doing so throughout a country's nuclear infrastructure.

---

[110] For a recent discussion of steps toward ensuring security for the long haul in Russia by a committee of the National Academy of Sciences, see Committee on Indigenization of Programs to Prevent Leakage of Plutonium and Highly Enriched Uranium from Russian Facilities, *Strengthening Long-Term Nuclear Security*. For an earlier discussion of sustainability in Russia and steps to achieve it, see Bukharin, Bunn, and Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union*. For a good discussion of the security culture issue in Russia, see Khripunov and Holmes, eds., *Nuclear Security Culture: The Case of Russia*.

Similarly, while some sites appear to have stronger security cultures in place than others, there continue to be reports of guards patrolling with no ammunition in their guns,[111] staff propping open security doors for convenience,[112] and guards turning off intrusion detectors when they become annoyed by the false alarms.[113] These events suggest that there is a good deal of work to do to achieve the level of commitment by all security-relevant staff needed for a truly effective nuclear security system.

DOE has recognized the challenge of ensuring sustainability and strong security cultures. With respect to sustainability, DOE is working to build up Russia's capability to sustain effective nuclear security. To provide the human capital needed to maintain an effective MPC&A system, it is providing extensive training programs. It is letting contracts to cover operations and maintenance costs for several years after new U.S.-funded equipment has been installed. DOE is also working to build up the infrastructure of firms and experts available for designing, building, installing, and maintaining nuclear security and accounting equipment in Russia. In addition to these efforts, DOE is helping Russia write and enforce effective nuclear security and accounting regulations, which, in principle, will still be forcing sites to take effective security measures long after U.S. assistance has come to an end. In one innovative and important move, DOE has negotiated contracts under which Russian facilities estimate their costs to maintain good nuclear security and accounting systems and lay out their plans for doing so.[114] Under the Bodman-Kirienko committee established at the Bratislava summit, DOE and Rosatom are now developing a joint sustainability plan, which explicitly includes the premise that U.S. resources devoted to nuclear security in Russia will decline year by year and will be replaced by increasing Russian resources. As of late 2006, however, that plan was not yet complete and agreed.[115] DOD is also planning a program to help ensure that the security measures it is financing at Russian nuclear warhead sites will be sustained, but this effort appears to be much smaller in scope, and public information about it is limited.

To build security culture, DOE and its Russian partners have included a focus on security culture in training programs. At a few Russian sites, they have also put in place "culture coordinators" on a pilot basis; these culture coordinators are comparable in some ways to the security awareness coordinators at DOE sites. After the Bratislava summit, where the two presidents emphasized the importance of security culture, efforts in this area have

---

[111] This practice, and many other issues that raise serious concerns about the effectiveness of the guard forces at Seversk (one of Russia's largest plutonium and HEU facilities) is described in Goloskokov, "Reforming MVD Troops to Guard Russian Nuclear Facilities [Translated]." At the time of the article, Goloskokov was the security chief for the Siberian Chemical Combine, the nuclear facility at Seversk.

[112] This is reported, with a photograph, in U.S. Congress, General Accounting Office, *Weapons of Mass Destruction: Additional Russian Cooperation Needed to Facilitate U.S. Efforts to Improve Security at Russian Sites*, GAO-03-482 (Washington, D.C.: GAO, 2003; available at http://www.gao.gov/new.items/d03482.pdf as of 4 March 2005).

[113] A number of Russian experts have reported this kind of incident to U.S. colleagues.

[114] For a brief discussion of DOE's current sustainability work, see U.S. Department of Energy, *2006 MPC&A Strategic Plan*.

[115] Interview with DOE official, December 2006.

been slowly expanding and Rosatom security officials have become more receptive.[116] In addition, DOE is sponsoring an "MPC&A Operations Monitoring" (MOM) project, in which security cameras are installed to monitor how personnel are doing their jobs at key locations, such as where staff are screened for nuclear material as they exit the building. This data provides site management (and potentially regulators) insights into the strengths and weaknesses of actual operations of the security systems. Awareness that they are being monitored gives personnel strong incentives to implement security procedures correctly. In some cases, the United States can even receive data from this monitoring – edited to remove any sensitive information – that give U.S. program managers additional insights on how systems are being operated and sustained. But there is still a great deal more to be done.

Sustainability. Steps like those taken thus far to improve sustainability and the security culture are essential, but are not likely to be sufficient. To achieve sustainability, two sets of recommendations above are likely to be especially important. Genuinely partnership-based approaches are essential: only if the experts at the sites using this equipment see it as having been in significant part their idea are they likely to have the necessary commitment to using, maintaining, and replacing it over time. Steps to convince political leaders and facility managers of the reality and urgency of the threat are equally critical, for those managers are only likely to devote the resources and sustained attention needed to maintain high levels of security if they genuinely believe that the threat is severe enough to require such measures.

Several additional steps are likely to be needed to get partner states to put in place the *resources*, *organizations*, and *incentives* essential to sustaining nuclear security for the long haul.

Resources. As a follow-up to the successful Bratislava summit initiative on nuclear security, President Bush should seek an explicit commitment from President Putin that he will assign sufficient resources from the Russian budget to ensure that security and accounting measures sufficient to defeat the threats that terrorists and thieves have demonstrated they can pose in Russia will be sustained after U.S. assistance phases out. Such a commitment should include some mechanism for following through, such as a specific line-item for nuclear security in the Russian state budget.

The possibility of creating a special fund for sustaining nuclear security should also be considered.[117] One possible mechanism would be for the United States and other partner countries to provide funding for sustainability projects that could only be used if matched by dedicated, transparent funds provided from the Russian state budget. At first an exact one-to-one match might not be necessary, but over time, the ratio of donor matching funds to

---

[116] Interviews with DOE officials and U.S. laboratory experts, October 2005 and July 2006.

[117] For a proposal for one particular approach to such a fund, see Committee on Indigenization of Programs to Prevent Leakage of Plutonium and Highly Enriched Uranium from Russian Facilities, *Strengthening Long-Term Nuclear Security*. For other approaches, see, for example, Matthew Bunn, John Holdren, and Anthony Wier, *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/securing_nuclear_weapons_and_materials_May2002.pdf as of 2 January 2007).

indigenous Russian funding should shift to reflect the increasing ability of Russia to secure its own nuclear warheads and materials against the threats terrorists have demonstrated they can pose. Such a matching fund would require mechanisms to show that work paid for was actually being completed.

Another source of revenue could be generated if, as part of negotiating arrangements for Russian commercial import of foreign spent fuel subject to U.S. veto rights, the United States insisted that an agreed portion of the revenue be put into a fund to support nuclear security. This would be Russia's own money, not U.S. taxpayer funds, and thus could be spent at highly sensitive sites and on other purposes for which the United States is not willing to allocate funds (such as actually paying the salaries of guards at nuclear sites) – but an agreed arrangement should be worked out to provide enough transparency to offer some confidence that the funds are indeed being spent on nuclear security.

As sustainability is not only a Russia problem, similar funding approaches should be considered with other partner countries with large-scale nuclear programs. For countries with only one or two nuclear facilities requiring high levels of security, more limited approaches to ensuring resources for sustainability are more likely to suffice.

Organizations. It will be extremely difficult to sustain effective nuclear security unless the organizations responsible have the personnel, expertise, resources, and authority to do so. The United States should work with Russia and other partner countries to ensure that every organization responsible for facilities with nuclear weapons or weapons-usable nuclear materials has a dedicated organization charged with ensuring effective security and accounting for those stockpiles and that every facility where these stockpiles are located has sufficient personnel, with sufficient resources and authority, dedicated to this mission.

The United States should put very high priority on working with partner countries to ensure that all nuclear regulatory bodies have the personnel, expertise, resources, and authority to write and enforce effective nuclear security and accounting rules. In some cases, this will mean going beyond providing training or equipment to regulatory bodies, to working with political leaders of partner countries to convince them to give their nuclear regulatory bodies enhanced authority or budgets. In the case of Russia, it will mean not only working to strengthen Rostekhnadzor (the regulator for all civilian nuclear activities in Russia) and Rosatom's internal regulation, but also working with the Ministry of Defense (MOD) regulatory group that in principle regulates security for all MOD nuclear activities and for those Rosatom activities involving nuclear weapons and components. Given the prominent role of the U.S. NRC in regulating nuclear security and accounting in the United States, NRC should be given the authority and budget to play a significant role in working with partner countries to set and enforce effective nuclear security and accounting rules.

Incentives. Every dollar a facility manager invests in security is a dollar not spent on something that would bring in revenue or accomplish the facility's core mission. It is essential to create strong incentives for nuclear security to counteract this obvious incentive to cut corners. Most facility managers simply will not make substantial investments in improving and maintaining security and accounting measures unless they have to. In many cases, "they have to" means that otherwise an inspector is going to come and find out that

they have not done so, and the result may be a fine, temporary closure, or something else they want to avoid. Hence, there could hardly be any subject more important to this entire agenda than effective nuclear security and accounting rules, effectively enforced. As noted above, a broad range of other steps can and should be taken to create and strengthen incentives for nuclear security.[118]

Consolidation. Finally, consolidating stockpiles of both nuclear warheads and weapons-usable nuclear materials into a much smaller number of sites (and a smaller number of buildings within those sites) is likely to be crucial to sustainability, because it will make it possible to achieve higher security at lower cost.

Security culture. As with sustainability, the steps above to build genuine nuclear security partnerships and to convince political leaders and facility managers of the urgency of threat are likely to be absolutely central to building effective security cultures. As already noted, the most fundamental element of an effective security culture is never forgetting to be afraid: the reality of the threat to be defended against needs to be inculcated constantly – in initial training, annual training, regular security exercises, and by any other means managers can think of. Convincing the top managers (and top security managers) of nuclear facilities is particularly important, for a strong security culture at a facility is only likely to get built if the facility management makes it a top mission to do so. Promoting an ongoing awareness of security incidents and trends around the world is also key, as only by being confronted with real data on ongoing incidents will people really be convinced about the scope and nature of the threats they need to defend against. Indeed, as noted above, tracking and forcing participants to confront such data on problems and near-misses, and the lessons drawn from them, has proven to be absolutely crucial to building effective *safety* cultures in industries throughout the world. As noted earlier, in the safety arena, management commitment and a good system for collecting and learning from such near-miss data are thought to be the two most important factors in achieving high levels of safety. Much the same is likely to be true for security.

Information and Intelligence to Support Policy

As the report of the commission on U.S. intelligence on weapons of mass destruction noted, good intelligence is crucial to the struggle to prevent nuclear terrorism, and this must be a top priority for U.S. intelligence agencies (and those of other countries as well) – but current U.S. intelligence in this area is weak.[119] Since 9/11, the level of U.S. intelligence focus on trying to figure out what terrorists might be doing related to weapons of mass destruction has increased substantially. But short of success in penetrating a cell working on

---

[118] Bunn, "Incentives for Nuclear Security."

[119] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President* (Washington, D.C.: WMD Commission, 2005; available at http://www.wmd.gov/report/ as of 2 January 2007).

weapons of mass destruction, it will always be very difficult to know what individual terrorist groups may be doing relating to weapons of mass destruction.[120]

Other kinds of information that are critical for policy-makers working this problem and are quite easy to get have not yet been given priority for collection and assessment (either by intelligence agencies or by policy and implementation agencies). How much are the workers paid at, for example, civilian research reactors with HEU? Is there corruption and theft among those workers? What are the conditions for the guard forces (if any)? What kind of terrorist and criminal activity has there been in the areas where these facilities are located, and what might that suggest about the threats that security at these facilities should be designed to cope with? This kind of information could be critical in assessing risks and setting priorities. Are particular reactors being used intensively, with plenty of funding, or are they used hardly at all and struggling to find the money to stay open? What do the officials in charge of providing the facilities' funding subsidies think about the possibility of shutting them down? What do the reactor operators think about the possibility of converting to low-enriched uranium? What do national policy-makers and facility operators think about the dangers of nuclear theft and sabotage and the security measures that should be taken to address them? This kind of information could be critical to identifying policy opportunities and obstacles. Comparable kinds of questions can and should be asked about a wide range of other types of facilities where nuclear weapons and materials exist as well.

Today, no one in the U.S. government (or other governments, as far as I am aware) has been given the task of collecting this type of information in a focused way on facilities with nuclear weapons or weapons-usable nuclear material throughout the world. To close that gap primarily requires simply reallocating current collection and analysis efforts, to focus on the issues that are most important to the problem that President Bush has identified as the most urgent national security threat to the United States.

The U.S. government should immediately develop and implement an interagency plan for collecting and analyzing the information most critical to assessing the risks of nuclear theft at sites throughout the world. In doing so, the U.S. government should be extraordinarily careful not to turn the experts attempting to build nuclear security partnerships with foreign colleagues into spies (or make them perceived to be spies), as that would destroy any hope of building the real partnerships that will be essential to success. In many cases, it may be that collection and analysis should *not* be done by intelligence agencies, but by implementation agencies or even by labs, companies, or universities on contract to the government; these entities can collect open information without the taint of U.S. government "spying."

A Prioritized Global Risk Assessment

Perhaps the first priority for information collection and analysis is a prioritized assessment of which facilities worldwide pose the most urgent risks of nuclear theft to be addressed, using the kinds of methodologies described in Chapter 4. DOE has developed a

[120] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President.*

list of facilities believed to have weapons-usable nuclear material around the world and is working to integrate what limited information is available about security arrangements and threats at these sites.[121] But to date, this list represents an inventory, not a risk-based assessment of where the highest priorities for action lie. Such a prioritized global threat assessment should be developed as quickly as possible – identifying not only what is known that gives reason for concern, but what is not known, and using those knowledge gaps to drive efforts to collect additional information to fill them. The record of past U.S. interactions with nuclear facilities should also be documented to the extent possible, so that U.S. officials are aware, in their discussions with facility operators, of what has gone before (DOE has in fact begun to populate the global facilities database with some information gleaned from previous interactions); in this way, judgments of where the highest-priority risks reside can be integrated with judgments concerning where the highest-leverage opportunities may be, or where higher-level political intervention may be needed to make progress.

A Long Road Yet to Travel

Real and important progress has been made in securing nuclear stockpiles in recent years, particularly in Russia. But there is more to be done there, and the effort in much of the rest of the world is just beginning. The steps recommended above could lead the way toward a faster, more effective, and more comprehensive effort to reduce the risks of nuclear theft and terrorism.

President Bush and President Putin, working with other world leaders, have the power to take actions that would transform the global effort to prevent nuclear terrorism. Between them, they have an historic opportunity to leave behind, as a lasting legacy, a world in which the danger of nuclear terrorism has been drastically reduced.

---

[121] Bunn and Wier, *Securing the Bomb: An Agenda for Action*, p. 103.

Bibliography

"5 Use Copter to Break out of Prison," *Los Angeles Times*, 31 December 2002.

"47th Annual Meeting of the Institute for Nuclear Materials Management," Nashville, Tenn, 16-20 July 2006.

"118 Hostages Are Dead in Moscow Theater Raid," *The Russia Journal*, 27 October 2002.

Agreement for Co-Operation between the Government of the United States of America and the Swiss Federal Council Concerning Peaceful Uses of Nuclear Energy (Washington, D.C.: U.S. Department of Energy, 1997; available at http://www.nnsa.doe.gov/na-20/docs/Switzerland_Agam.pdf as of 19 July 2005).

Amendment to the Convention on the Physical Protection of Nuclear Material (Vienna: International Atomic Energy Agency, 2005; available at http://www-pub.iaea.org/MTCD/Meetings/ccpnmdocs/cppnm_proposal.pdf as of 16 September 2005).

"Annex: Attributes of Proliferation Resistance for Civilian Nuclear Power Systems," in *Technological Opportunities to Increase the Proliferation Resistance of Global Nuclear Power Systems (TOPS)* (Washington, D.C.: U.S. Department of Energy, Nuclear Energy Research Advisory Committee, 2000; available at http://www.nuclear.gov/nerac/FinalTOPSRptAnnex.pdf as of 9 January 2007).

Assessing the G8 Global Partnership: From Kananaskis to St. Petersburg (Washington, D.C.: Strengthening the Global Partnership Project, Center for Strategic and International Studies, 2006; available at http://www.sgpproject.org/publications/SGPAssessment2006.pdf as of 22 December 2006).

Atomic Energy Act of 1954, as Amended (Washington, D.C.: Government Printing Office, 1954; available at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0980/ml022200075-vol1.pdf as of 22 December 2006).

"Aum Cult May Possess Plans on Overseas Nuclear Plants," *Kyodo News Service*, 27 March 2000.

"Business Breakfast [Interview with Col.-Gen. Alexander Savenkov]," trans. BBC Monitoring, *Rossiskaya Gazeta*, 27 December 2003.

"Chart of Nuclides" (Upton, N.Y.: Brookhaven National Laboratory, 2006; available at http://www.nndc.bnl.gov/chart/ as of 9 January 2007).

"Chechen Rebel Says Will Never Ask Russia for Peace," *Reuters*, 16 May 2005.

"Confirmed Proliferation-Significant Incidents of Fissile Material Trafficking in the Newly Independent States (NIS), 1991-2001" (Monterey, Cal.: Center for Nonproliferation

Studies, Monterey Institute of International Studies, 30 November 2001; available at http://cns.miis.edu/pubs/reports/traff.htm as of 3 March 2006).

Committee on Science, Space, and Technology, *Conversion of Research and Test Reactors to Low-Enriched Uranium (LEU) Fuel*, U.S. Congress, House of Representatives, 98th Congress, 2nd Session, 25 September 1984.

"Cult Siphoned Nuclear Data," *Asahi News Service*, 29 March 2000.

Committee on Armed Services, *Current and Future Worldwide Threats to the National Security of the United States*, U.S. Senate, 108th Congress, 2nd Session, 9 March 2004.

Select Committee on Intelligence, *Current and Projected National Security Threats to the United States*, U.S. Senate, 109th Congress, 16 February 2005 (available at http://www.fas.org/irp/congress/2005_hr/shrg109-61.pdf as of 4 January 2007).

Select Committee on Intelligence, *Current and Projected National Security Threats to the United States*, U.S. Senate, 108th Congress, 2nd Session, 24 February 2004 (available at http://intelligence.senate.gov/0402hrg/040224/witness.htm as of 28 February 2006).

"'Enormous Damage' from Equipment Theft in Russian Navy," trans. BBC Monitoring Service, *RTR-TV (Moscow)*, 6 December 2003.

"Escaped Musharraf Plotter Was Pakistan Air Force Man," *Agence France Presse*, 12 January 2005.

"Exclusive Interview with Dr. Abdul Qadeer Khan (Excerpts)," trans. BBC Summary of World Broadcasts, *Nawa-e Waqt*, 10 February 1984.

"Fact Sheet: Project Vinca" (Washington, D.C.: U.S. Department of State, 23 August 2002; available at http://www.state.gov/r/pa/prs/ps/2002/12962.htm as of 28 September 2005).

"The First Bush-Kerry Presidential Debate, University of Miami, Coral Gables, Florida," *Commission on Presidential Debates*, 30 September 2004.

"French Air Force Installs Radar System at Nuclear Site," *Agence France-Presse*, 19 October 2001.

"Frontline: Loose Nukes: Interviews" (Public Broadcasting System, 1996; available at http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/ as of 22 December 2005).

"The G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction" (Kananaskis, Canada: Government of Canada, 27 June 2002; available at http://www.g7.utoronto.ca/summit/2002kananaskis/arms.html as of 27 June 2006).

Committee on Appropriations, Subcommittee on Energy and Water, *Global Nuclear Energy Partnership*, U.S. Senate, 109th Congress, 2nd Session, 14 September 2006.

Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction, Part II*, U.S. Senate, 104th Congress, 2nd Session, 13, 20, and 22 March 1996.

"Government of Kazakhstan and NTI Mark Success of HEU Blend-Down Project: Material Could Have Been Used to Make up to Two Dozen Nuclear Bombs" (Ust-Kamenogorsk, Kazakhstan: Nuclear Threat Initiative, 8 October 2005; available at http://www.nti.org/c_press/release_Kaz_100805.pdf as of 17 December 2005).

"The Great Diamond Heist," "PrimeTime Live," *ABC News*, 12 February 2005.

National Security Committee, Military Research & Development Subcommittee, *Hearing on Russian Missile Detargeting and Nuclear Doctrine and Its Relation to National Missile Defense*, U.S. House of Representatives, 105th Congress, 1st Session, 13 March 1997 (available at http://armedservices.house.gov/testimony/105thcongress/97-3-13Blair.htm as of 28 February 2006).

House Committee on Energy and Commerce, Energy and Air Quality Subcommittee, *A Hearing to Review Proposals to Consolidate the Offices of Counter Intelligence at NNSA and DOE*, 13 July 2004 (available at http://energycommerce.house.gov/108/Hearings/07132004hearing1346/hearing.htm as of 15 August 2005).

"Internal Troops to Make Russian State Facilities Less Vulnerable to Terrorists," *RIA-Novosti*, 5 October 2005.

International Convention for the Suppression of Acts of Nuclear Terrorism (New York: United Nations, 2005; available at http://www.un.int/usa/a-59-766.pdf as of 16 September 2005).

"Interview with Khidhir Hamza" in *Frontline: Gunning for Saddam*, ed. (Washington, D.C.: Public Broadcasting System, 2001; available at http://www.pbs.org/wgbh/pages/frontline/shows/gunning/interviews/hamza.html as of 10 December 2006).

"Interview: Victor Yerastov: Minatom Has All Conditions for Providing Safety and Security of Nuclear Material," *Yaderny Kontrol Digest* 5, no. 1 (Winter 2000).

"Japanese Police Issue Annual Report Stressing Threat of Terrorism, Cults," *Kyodo News Service*, 7 December 2004.

"Joint Statement by U.S. President George Bush and Russian Federation President V.V. Putin Announcing the Global Initiative to Combat Nuclear Terrorism" (St. Petersburg, Russia: The White House, Office of the Press Secretary, 15 July 2006; available at http://www.whitehouse.gov/news/releases/2006/07/20060715-2.html as of 22 December 2006).

"Joint Statement on New U.S.-Russian Relationship" (Crawford, Texas: The White House, Office of the Press Secretary, 13 November 2001; available at http://www.whitehouse.gov/news/releases/2001/11/20011113-4.html as of 22 August 2005).

Committee on Foreign Relations, Subcommittee on European Affairs

Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Loose Nukes, Nuclear Smuggling, and the Fissile Material Problem in Russia and the NIS*, U.S. Senate, 104th Congress, 1st Session, 22-23 August 1995.

"Musharraf Al-Qaeda Revelation Underlines Vulnerability: Analysts," *Agence France Presse*, 31 May 2004.

"Nachalnik Operativnogo Shtaba Maskhadova Gotovil Plan Zakhvata Rosiiskoi Atomnoi Podlodki (Chief of Maskhadov's Operational Staff Was Preparing a Plan to Hijack Russian Atomic Submarine)," *RIA-Novosti*, 25 April 2002.

Committee on Science, *NASA's Organizational and Management Challenge*, U.S. Congress, House of Representatives, 29 October 2003.

National Planning Scenarios (Washington, D.C.: U.S. Department of Homeland Security, 2005; available at http://media.washingtonpost.com/wp-srv/nation/nationalsecurity/earlywarning/NationalPlanningScenariosApril2005.pdf as of 4 October 2005).

"NIS Nuclear Trafficking Database" (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2006; available at http://www.nti.org/db/nistraff/ as of 12 December 2006).

"Not a Tin Soldier; Chief Military Prosecutor Comments on Investigation of Sensational Military Crimes," trans. BBC Monitoring, *Rossiskaya Gazeta*, 24 December 2003.

"Nuclear Center Worker Caught Selling Secrets," trans. BBC Summary of World Broadcasts, *Russian NTV*, 18 December 1998.

Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Nuclear Security Coverup*, U.S. Congress, House of Representatives, 98th Congress, 2nd Session, 3 February 1984.

"Nuclear Security Hiked against Chechen Threat," *Moscow Times*, 21 February 2003.

Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, *Nuclear Security: Has the NRC Strengthened Facility Standards since 9/11?* U.S. House of Representatives, 109th Congress, 2nd Session, 4 April 2006 (available at http://reform.house.gov/NSETIR/Hearings/EventSingle.aspx?EventID=41937 as of 6 May 2006).

"Nuclear Storage Facility Commissioned in Russia's Chelyabinsk Region," *ITAR-TASS*, 11 July 2006.

Committee on Energy and Commerce, *Nuclear Weapons Facilities: Adequacy of Safeguards and Security at Department of Energy Nuclear Weapons Production Facilities*, U.S. Congress, House of Representatives, 99th Congress, 2nd Session, 6 March 1986.

"Over 4,000 Trespassers Detained at Moscow District Restricted Access Facilities," *Interfax-Agentstvo Voyennykh Novostey*, 18 March 2005.

"Physical Protection Upgrades for the Uzbekistan VVR-SM Reactor," *International Security News* 2, no. 2 (May 2002; available at www.cmc.sandia.gov/isn/may02isn.pdf as of 22 November 2006), pp. 14-15.

Plan Meropriyatii, Cvyazannykh S Vypolneniem Pervogo Etapa Pealizatsii 'Osnov Gosudarstvennoi Politiki V Oblast'i Obespecheniya Yadernoi I Radiatsionnoi Bezopasnost'i Rossiskoi Federatsii Na Period Do 2010 Goda I Dal'neishuyu Perspektivu' (Action Plan for Phase One of the Implementation of 'Foundations of Government Policy in the Area of Nuclear Safety and Radiation Protection within the Russian Federation for the Period to 2010 and Beyond'), trans. U.S. Department of Energy, Order No. 117-r (Moscow: Government of the Russian Federation, 2005; available at http://www.government.ru/data/news_text.html?he_id=103&news_id=16586 as of 25 February 2005).

"Plutonium Con Artists Sentenced in Russian Closed City of Sarov," *NIS Export Control Observer* (November 2003; available at http://cns.miis.edu/pubs/nisexcon/pdfs/ob_0311e.pdf as of 23 December 2006).

Subcommittee on Strategic Forces, Committee on Armed Services, *Plutonium Disposition and the U.S. Mixed Oxide Fuel Facility*, U.S. House of Representatives, 109th Congress, 2nd Session, 26 July 2006 (available at http://www.house.gov/hasc/schedules/ as of 10 August 2006).

"Race against Time to Prevent Nuclear Terror - IAEA," *Reuters*, 8 November 2004.

"Radioactive Device Stolen from Halliburton India Unit," *Dow Jones Newswires*, 11 October 1993.

"Radioactive Material Stolen from Steel Plant in Eastern India," *Associated Press Newswires*, 17 August 2003.

"Radioactive Road Trip," "PrimeTime Live," *ABC News*, 13 October 2005.

Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *A Review of Security Initiatives at DOE Nuclear Facilities*, U.S. Congress, House of Representatives, 109th Congress, 1st Session, 18 March 2005 (available at http://energycommerce.house.gov/108/Hearings/03182005hearing1457/hearing.htm as of 15 August 2005).

"Russia: Criminals Indicted for Selling Mercury as Weapons-Grade Plutonium," trans. U.S. Department of Commerce, *Izvestiya*, 11 October 2003.

"Russia: Terror Groups Scoped Nuke Site," *Associated Press*, 25 October 2001.

"Russian Court Sentences Men for Weapons-Grade Plutonium Scam," trans. BBC Monitoring Service, *RIA Novosti*, 14 October 2003.

"Russian TV Says Chechen Rebels Plotted to Seize Nuclear Submarine.," *Interfax*, 27 April 2002.

"Saddam's Bombmaker," "60 Minutes II," *CBS News*, 27 January 1999.

"Secret Mission to Recover Highly Enriched Uranium in Uzbekistan Successful: Fuel Returned to Secure Facility in Russia" (Washington, D.C.: U.S. Department of Energy, 13 September 2004; available at http://www.energy.gov as of 16 February 2005).

"Security Agency Inspects 39 Aum-Linked Facilities in 2004," *Kyodo News Service*, 22 April 2005.

"Statement of Principles by Participants in the Global Initiative to Combat Nuclear Terrorism" (Washington, D.C.: The White House, Office of the Press Secretary, 31 October 2006; available at http://www.state.gov/r/pa/prs/ps/2006/75405.htm as of 22 December 2006).

"Statement on Nuclear Security Cooperation with Russia" (Washington, D.C.: The White House, Office of the Press Secretary, 30 June 2005; available at http://www.whitehouse.gov/news/releases/2005/06/20050630-4.html as of 7 July 2005).

The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, INFCIRC/153 (Corrected) (Vienna: International Atomic Energy Agency, 1972; available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf153.shtml as of 22 August 2005).

Swift Knight -- Usam Ben Laden's Current and Historical Activities (1998; available at http://www.judicialwatch.org/cases/102/dia.pdf as of 8 December 2006).

"Systems under Fire," *U.S. Department of Energy, Office of Independent Oversight and Performance Assurance*, 2003.

"Taliban Tries to Access Nuclear Technologies - Russian Security Council Official," *Interfax*, 7 October 2000.

"Text: Excerpts of Reuters Interview with Chechen Rebel Leader," *Reuters*, 18 July 2004.

"Text: US Grand Jury Indictment against Usama Bin Laden" (New York: United States District Court, Southern District of New York, 6 November 1998; available at http://www.fas.org/irp/news/1998/11/98110602_nlt.html as of 4 April 2006).

"Three Pinch Valves Were Stolen from the Leningrad Nuclear Power Plant, Abstract 20040380," in *Nuclear Threat Initiative Research Library: NIS Trafficking Database* (Monterey, Cal.: Monterey Institute for International Studies, Center for Nonproliferation Studies, 2004; available at http://www.nti.org/db/nistraff/2004/20040380.htm as of 28 February 2005).

"Top Russian Official Does Not Rule out International Terrorists May Obtain Nuclear Materials," *Interfax News Service*, 18 September 2004.

Committee on the Judiciary, *United States Department of Justice*, U.S. House of Representatives, 108th Congress, 1st Session, 5 June 2003 (available at http://judiciary.house.gov/media/pdfs/printers/108th/87536.PDF as of 4 April 2006).

Committee on Foreign Relations, *An Update on North Korean Nuclear Developments*, U.S. Senate, 108th Congress, 2nd Session, 21 January 2004 (available at http://www.senate.gov/~foreign/hearings/2004/hrg040121a.html as of 9 August 2006).

"US Money Lost on Way to Former Russian Army Servicemen," trans. BBC Monitoring Service, *Ekho Moskvy*, 15 February 2005.

"'We Cannot Preclude the Possibility of Nuclear Materials Theft' (Edited Transcript of Duma Hearing)," *Yaderny Kontrol Digest* 5 (Fall 1997).

"'Why We Fight America': Al-Qa'ida Spokesman Explains September 11 and Declares Intentions to Kill 4 Million Americans with Weapons of Mass Destruction," *MEMRI (Middle East Media Research Institute) Special Dispatch*, no. 388 (2002; available at http://memri.org/bin/articles.cgi?Page=archives&Area=sd&ID=SP38802 as of 4 April 2006).

Abraham, Spencer, "International Atomic Energy Agency, Vienna: Remarks Prepared for Energy Secretary Spencer Abraham" (Washington, D.C.: U.S. Department of Energy, 26 May 2004; available at http://www.energy.gov/news/1800.htm as of 12 May 2006).

Afzal, Muhammad, "Cooperation in Fissile Material Management: The View from Pakistan," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

Albright, David, "Al Qaeda's Nuclear Program: Through the Window of Seized Documents," *Nautilus Institute Special Forum* 47 (2002; available at http://www.nautilus.org/archives/fora/Special-Policy-Forum/47_Albright.html as of 2 January 2007).

----------, *Iraq's Programs to Make Highly Enriched Uranium and Plutonium for Nuclear Weapons Prior to the Gulf War* (Washington, D.C.: Institute for Science and International Security, 2002; available at http://www.isis-online.org/publications/iraq/iraqs_fm_history.html as of 10 December 2006).

----------, *Shipments of Weapons-Usable Plutonium in the Commercial Nuclear Industry* (Washington, D.C.: Institute for Science and International Security, 2007; available

at http://www.isis-online.org/global_stocks/end2003/plutonium_shipments.pdf as of 3 January 2007).

----------, "South Africa and the Affordable Bomb," *Bulletin of the Atomic Scientists* 50, no. 4 (1994; available at http://www.thebulletin.org/article.php?art_ofn=ja94albright as of 28 February 2006).

----------, "When Could Iran Get the Bomb?" *Bulletin of the Atomic Scientists* 62, no. 4 (July/August 2006; available at http://www.thebulletin.org/article.php?art_ofn=ja06albright as of 5 December 2006), pp. 26-33.

Albright, David, and Lauren Barbour, "Troubles Tomorrow? Separated Neptunium-237 and Americium," in *The Challenges of Fissile Material Control*, ed. David Albright and Kevin O'Neill (Washington, D.C.: Institute for Science and International Security, 1999; available at http://www.isis-online.org/publications/fmct/book/New%20chapter%205.pdf as of 11 January 2007).

Albright, David, Frans Berkhout, and William B. Walker, *Plutonium and Highly Enriched Uranium, 1996: World Inventories, Capabilities, and Policies* (Solna, Sweden; Oxford, UK; and New York: Stockholm International Peace Research Institute (SIPRI) and Oxford University Press, 1996).

Albright, David, and Paul Brannan, "The North Korean Plutonium Stock, Mid-2006" (Washington, D.C.: Institute for Science and International Security, 26 June 2006; available at http://www.isis-online.org/publications/dprk/dprkplutonium.pdf as of 13 August 2006).

Albright, David, Kathryn Buehler, and Holly Higgins, "Bin Laden and the Bomb," *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.isis-online.org/publications/terrorism/binladenandbomb.pdf as of 2 January 2007), pp. 23-24.

Albright, David, and Khidhir Hamza, "Iraq's Reconstitution of Its Nuclear Weapons Program," *Arms Control Today* 28 (October 1998; available at http://www.armscontrol.org/act/1998_10/daoc98.asp as of 27 February 2006).

Albright, David, and Holly Higgins, "A Bomb for the Ummah," *Bulletin of the Atomic Scientists* 59, no. 2 (March/April 2003; available at http://www.thebulletin.org/issues/2003/ma03/ma03albright.html as of 2 January 2007), pp. 49-55.

Albright, David, and Corey Hinderstein, "Iran's Next Steps: Final Tests and the Construction of a Uranium Enrichment Plant" (Washington, D.C.: Institute for Science and International Security, 12 January 2006; available at http://www.isis-online.org/publications/iran/irancascade.pdf as of 6 April 2006).

----------, "Unraveling the A.Q. Khan and Future Proliferation Networks," *Washington Quarterly* 28, no. 2 (Spring 2005; available at http://www.twq.com/05spring/docs/05spring_albright.pdf as of 1 August 2005).

Albright, David, and Kimberly Kramer, "Civil HEU Watch: Tracking Inventories of Civil Highly Enriched Uranium," in *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, 2005; available at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html as of 21 July 2005).

----------, eds., *Global Fissile Material Inventories* (Washington, D.C.: Institute for Science and International Security, 2004; available at http://www.isis-online.org/global_stocks/tableofcontents.html as of 14 February 2005).

----------, "Plutonium Watch: Tracking Civil Plutonium Inventories," in *Global Stocks of Nuclear Explosive Materials* (Washington, D.C.: Institute for Science and International Security, 2005; available at http://www.isis-online.org/global_stocks/end2003/tableofcontents.html as of 21 July 2005).

Albright, Madeleine, "Arms Control in the 21st Century" (Washington, D.C.: U.S. Department of State, 10 June 1998; available at http://www.clw.org/archive/coalition/albr0610.htm as of 9 May 2006).

Allison, Graham, Ashton B. Carter, Steven E. Miller, and Philip Zelikow, *Cooperative Denuclearization: From Pledges to Deeds* (Cambridge, MA: Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 1993).

Allison, Graham T., *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004).

Allison, Graham T., Owen R. Cote, Richard A. Falkenrath, and Steven E. Miller, *Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nulcear Weapons and Fissile Material* (Cambridge, MA: MIT Press, 1996).

Altman, W., J. Hockert, and E. Quinn, *A Safeguards Case Study of the Nuclear Materials and Equipment Corporation Uranium Processing Plant: Apollo, Pennsylvania*, vol. NUREG-0627 (Washington, DC.: U.S. Nuclear Regulatory Commission, 1979).

Alvarez, Luis, *Adventures of a Physicist* (New York: Basic Books, 1987).

Andes, Trent, "Sample Appendix a for Generic MTR Assembly," in *IAEA/USA Interregional Training Course: Technical and Administrative Preparations Required for Shipment of Research Reactor Spent Fuel to Its Country of Origin, 13-24 January 1997, Argonne, Ill.* (Argonne, Ill.: Argonne National Laboratory, 1997; available at http://www.rertr.anl.gov/IAEA197/sampl31a.html as of 20 September 2006).

Annan, Kofi, "A Global Strategy for Fighting Terrorism: Keynote Address to the Closing Plenary," in *The International Summit on Democracy, Terrorism and Security* (Madrid: Club de Madrid, 2005; available at http://english.safe-democracy.org/keynotes/a-global-strategy-for-fighting-terrorism.html as of 10 March 2005).

Anonymous, *Through Our Enemies' Eyes: Osama Bin Laden, Radical Islam, and the Future of America* (Washington, D.C.: Brassey's, 2002).

Anonymous [Michael Scheuer], "How Not to Catch a Terrorist," *Atlantic Monthly* 294, no. 5 (2004; available at http://www.theatlantic.com/doc/200412/anonymous as of 5 January 2007), p. 50.

Aoyama, Shin, "Current Nuclear Physical Protection Measures in Japan," paper presented at Seminar on Strengthening Nuclear Security in Asian Countries, Tokyo, 8-9 November 2006.

Apostolakis, George E., "How Useful Is Quantitative Risk Assessment?" *Risk Analysis* 24, no. 3 (2004).

Applegarth, Christina, "Russia, U.S. Bolster Regional Nuclear Security Following Terrorist Attacks," *Arms Control Today* (October 2004; available at http://www.armscontrol.org/act/2004_10/GTRI.asp as of 5 April 2006).

Arbman, Gunnar, and Charles Thornton, *Russia's Tactical Nuclear Weapons: Part I: Background and Policy Issues*, vol. FOI-R--1057--SE (Stockholm: Swedish Defense Research Agency, 2003).

----------, *Russia's Tactical Nuclear Weapons: Part II: Technical Issues and Policy Recommendations*, vol. FOI-R—1588—SE (Stockholm: Swedish Defense Research Agency, 2005; available at http://www.foi.se/upload/pdf/FOI-RussiasTacticalNuclearWeapons.pdf as of 12 April 2005).

Arkin, William M., and Richard W. Fieldhouse, *Nuclear Battlefields: Global Links in the Arms Race* (Cambridge, Mass.: Ballinger, 1985).

Avdeyev, Sergei, "Chechens Gain Access to Nuclear Warheads," *Izvestia*, 22 March 2002.

Avedon, Roger E., "On the Future of Civilian Plutonium: An Assessment of Technological Impediments to Nuclear Terrorism and Proliferation" (Ph.D. dissertation, Engineering Economic Systems and Operations Research, Stanford, 1997).

Bagrov, Yuri, "Cache of Unprotected Radioactive Material Found in Chechnya," *Associated Press*, 16 April 2003.

Bailey, Emily, Richard Guthrie, Darryl Howlett, and John Simpson, eds., *Briefing Book: Volume II: Treaties, Agreements, and Other Relevant Documents* (Southampton, U.K.: Programme for Promoting Nuclear Non-Proliferation, 2000).

Baker, Peter, "Pakistani Scientist Who Met Bin Laden Failed Polygraphs, Renewing Suspicions," *Washington Post*, 3 March 2002.

Baker, Peter, and Susan B. Glasser, "Russian Plane Bombers Exploited Corrupt System," *Washington Post*, 18 September 2004.

Baker, Richard S., Siegried S. Hecker, and Delbert R. Harbur, "Plutonium: A Wartime Nightmare but a Metallurgist's Dream," *Los Alamos Science* (Winter/Spring 1983; available at http://www.fas.org/sgp/othergov/doe/lanl/pubs/00416629.pdf as of 19 September 2006).

Ballard, Tim, Jason Pate, Gary Ackerman, Diana McCauley, and Sean Lawson, *Chronology of Aum Shinrikyo's Cbw Activities* (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2001; available at http://www.cns.miis.edu/pubs/reports/aum_chrn.htm as of 2 January 2007).

Barnaby, Frank, *How to Build a Nuclear Bomb and Other Weapons of Mass Destruction* (New York: Nation Books, 2004).

Bazerman, Max H., and Michael D. Watkins, *Predictable Surprises: The Disasters You Should Have Seen Coming and How to Prevent Them* (Cambridge, Mass.: Harvard Business School Publishing, 2004).

Bell, Rachel, "Sensational Heists," in *Crime Library* (Court TV, 2005; available at http://www.crimelibrary.com/gangsters_outlaws/outlaws/major_heists/index.html#continue as of 22 December 2005).

Benedict, Manson, Thomas H. Pigford, and Hans Wolfgang Levi, *Nuclear Chemical Engineering*, 2nd ed. (New York: McGraw-Hill, 1981).

Benjamin, Daniel, and Steven Simon, *The Next Attack: The Failure of the War on Terror and a Strategy for Getting It Right* (New York: Times Books, 2005).

Bergen, Peter L., *Holy War, Inc.: Inside the Secret World of Osama Bin Laden*, updated edition ed. (New York: Touchstone, 2002).

Biden, Joseph, "Avoiding Nuclear Anarchy," in *The Paul C. Warnke Conference on the Past, Present, and Future of Arms Control, Georgetown University, Washington, D.C.*, (Washington, D.C.: Arms Control Association, Edmund A. Walsh School of Foreign Service, and Center for Peace and Security Studies, 2004; available at http://www.armscontrol.org/PDF/WarnkePDFTranscript.pdf as of 12 December 2006).

Bisaeva, Amina, "Chechnya's Ticking Radiation Bomb," *Environment News Service*, 27 January 2005 (available at http://www.ens-newswire.com/ens/jan2005/2005-01-27-01.asp as of 2 December 2006).

Bleek, Philipp C., *Global Cleanout: An Emerging Approach to the Civil Nuclear Material Threat* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2004; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/bleekglobalcleanout.pdf as of 13 April 2005).

----------, "Project Vinca: Lessons for Securing Civil Nuclear Material Stockpiles," *Nonproliferation Review* (Fall-Winter 2003; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/NonProRev-Bleek.pdf as of 28 September 2005).

BNFL National Stakeholder Dialogue, Security Working Group, *Final Report* (London: The Environment Council, 2004).

BNFL National Stakeholder Dialogue, Waste Working Group, *Interim Report* (London: Environmental Council, 2000; available at http://www.the-environment-council.org.uk/docs/WWG%20Combined%20Report.pdf as of 4 August 2005).

Bodman, Samuel, "Carnegie Endowment for International Peace Moscow Center: Remarks as Prepared for Secretary Bodman" (Moscow: U.S. Department of Energy, 16 March 2006; available at http://energy.gov/news/3348.htm as of 29 December 2006).

Bogdanov, Vladimir, "Propusk K Beogolovkam Nashli U Terrorista (a Pass to Warheads Found on a Terrorist)," *Rossiskaya Gazeta*, 1 November 2002.

Boutwell, Jeffrey, Francesco Calogero, and Jack Harris, "Nuclear Terrorism: The Danger of Highly Enriched Uranium," *Pugwash Issue Briefs* 2, no. 1 (September 2002; available at http://www.pugwash.org/publication/pb/sept2002.pdf as of 3 April 2006).

Bowers, Faye, "Eavesdropping on Terror Talk in Germany," *Christian Science Monitor*, 28 January 2005.

Braun, Chaim, and Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime," *International Security* 29, no. 2 (Fall 2004; available at http://iis-db.stanford.edu/pubs/20716/braun-chyba-is-fall04.pdf as of 1 August 2005).

Bremer Maerli, Morton, "U.S.-Russian Naval Security Upgrades: Lessons Learned and the Way Ahead," *Naval War College Review* 56, no. 4 (Autumn 2003; available at http://www.nwc.navy.mil/press/Review/2003/Autumn/pdfs/art2-a03.pdf as of 18 April 2005).

Brian, Danielle, and Peter Stockton, "POGO Presentation to NRC Security Inspectors" (Washington, D.C.: Project on Government Oversight, 16 December 2004; available at http://pogo.org/m/hsp/hsp-NRCPhysSecInsp-041216.pdf as of 5 January 2007).

Broad, William J., "Libya's Crude Bomb Design Eases Western Experts' Fear," *New York Times*, 9 February 2004.

Brouse, C., J. Aurelle, R. Venot, and J. Jalouneix, "IRSN Activities in Physical Protection in Support of the IAEA: The Insider Threats Approach," in *Eurosafe Forum 2003: Paris, 25-26 November* (Paris: Eurosafe Forum, 2003; available at http://www.eurosafe-forum.org/products/data/5/pe_190_24_1_5_9paper.pdf as of 30 July 2006).

Brundson, William C., "Nuclear Terrorism Risk Reduction: Evaluating the Effectiveness of the Department of Energy's United States/Russian Nuclear Material Protection, Control, and Accounting (MPC&A) Program" (Ph.D. dissertation, Graduate School of International Studies, University of Denver, 2005).

Bryanski, Gleb, "Interview: Chechens Could Strike Nuclear Plant Next," *Reuters*, 27 October 2002.

Bukharin, Oleg, "Physical Protection Performance Testing: Assessing U.S. NRC Experience," *Journal of Nuclear Materials Management* 28, no. 4 (Summer 2000).

----------, *Russia's Nuclear Complex: Surviving the End of the Cold War* (Princeton, N.J.: Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2004; available at http://www.ransac.org/PDFFrameset.asp?PDF=bukharinminatomsurvivalmay2004.pdf as of 8 March 2005).

----------, *Russia's Gaseous Centrifuge Technology and Uranium Enrichment Complex* (Princeton, N.J.: Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2004).

----------, "Security of Fissile Materials in Russia," *Annual Review of Energy and the Environment* 21 (1996).

Bukharin, Oleg, Matthew Bunn, and Kenneth N. Luongo, *Renewing the Partnership: Recommendations for Accelerated Action to Secure Nuclear Material in the Former Soviet Union* (Washington, D.C.: Russian American Nuclear Security Advisory Council, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mpca2000.pdf as of 2 January 2007).

Bukharin, Oleg, and William Potter, "Potatoes Were Guarded Better," *Bulletin of the Atomic Scientists* 51, no. 3 (May-June 1995), pp. 46-50.

Bunn, George, "Raising International Standards for Protecting Nuclear Materials from Theft and Sabotage," *Nonproliferation Review* 7, no. 2 (Summer 2000; available at http://cns.miis.edu/pubs/npr/vol07/72/72bunn.pdf as of 2 January 2007).

Bunn, George, Chaim Braun, Alexander Glaser, Edwin Lyman, and Fritz Steinhausler, "Research Reactor Vulnerability to Sabotage by Terrorists," *Science and Global Security* 11 (2003; available at http://www.princeton.edu/~globsec/publications/pdf/11%202-3%20Bunn%20p85-107.pdf as of 2 January 2007).

Bunn, George, and Lyudmila Zaitseva, "Guarding Nuclear Reactors and Materials from Terrorists and Thieves," in *IAEA Symposium on International Safeguards: Verification & Nuclear Material Security* (Vienna: International Atomic Energy Agency, 2001; available at http://www.iaea.org/worldatom/Meetings/2001/infsm367progr_fr.shtml as of 13 June 2006).

Bunn, Matthew, "Anecdotes of Insecurity," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/threat/anecdote.asp as of 2 January 2007).

----------, "Building a Genuine U.S.-Russian Partnership for Nuclear Security," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Phoenix, Ariz.: INMM, 2005; available at http://bcsia.ksg.harvard.edu/BCSIA_content_stage/documents/inmmpartnership205.pdf as of 2 January 2007).

----------, "Cooperation to Secure Nuclear Stockpiles: A Case of Constrained Innovation," *Innovations* 1, no. 1 (2006; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/INNOV0101_CooperationtoSecureNuclearStockpiles.pdf as of 4 April 2006).

----------, "Fissile Material Cutoff Treaty," in *Nuclear Threat Initiative Research Library: Securing the Bomb*, ed. Matthew Bunn and Anthony Wier (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/ending/fmct.asp as of 2 January 2007).

----------, "IAEA Monitoring of Excess Nuclear Material," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/monitoring/trilateral.asp as of 23 May 2006).

----------, "Incentives for Nuclear Security," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

----------, "Mayak Fissile Material Storage Facility," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/cnwm/securing/mayak.asp as of 2 January 2007).

----------, *The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material* (Washington, D.C.: Managing the Atom Project, Harvard University, and Non-Proliferation Project, Carnegie Endowment for International Peace, 2000; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/FullNextWave.pdf as of 2 January 2007).

----------, "Nuclear Security in the United States: Response to 9/11" (unpublished: 3 February 2005).

----------, "Systems Approaches to Security for Nuclear Materials and Facilities", *Presentation, "Research Seminar in Engineering Systems," Massachusetts Institute of Technology* (Cambridge, Mass.: Managing the Atom Project, Harvard University, 4 December 2001).

----------, "The Threat in Russia and the Newly Independent States," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2006; available at http://www.nti.org/e_research/cnwm/threat/russia.asp as of 2 January 2007).

----------, "UNSC 1540: Next Steps to Seize the Opportunity," paper presented at A New Role for the United Nations Security Council: Criminalizing WMD Proliferation--The Impact of U.N. Security Council Resolution 1540, Arlington, Va., 15 March 2005 (available

at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/UNSC1540.pdf as of 2 January 2007).

Bunn, Matthew, and John P. Holdren, "Managing Military Uranium and Plutonium in the United States and the Former Soviet Union," *Annual Review of Energy & the Environment* 22, no. 1 (1997; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/mmup.pdf as of 6 February 2006).

Bunn, Matthew, John Holdren, and Anthony Wier, *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/securing_nuclear_weapons_and_materials_May2002.pdf as of 2 January 2007).

Bunn, Matthew, and Anthony Wier, with Joshua Friedman, "The Demand for Black Market Fissile Material," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/cnwm/threat/demand.asp as of 2 January 2007).

----------, *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative; available at http://www.nti.org/securingthebomb as of 3 April 2006).

----------, *Securing the Bomb 2005: The New Global Imperatives* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2005; available at http://www.nti.org/e_research/report_cnwmupdate2005.pdf as of 2 January 2007).

----------, *Securing the Bomb 2006* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2006; available at http://www.nti.org/securingthebomb as of 23 July 2006).

----------, *Securing the Bomb: An Agenda for Action* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2004; available at http://www.nti.org/e_research/analysis_cnwmupdate_052404.pdf as of 2 January 2007).

Bunn, Matthew, Anthony Wier, and John Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2003; available at http://www.nti.org/e_research/cnwm/cnwm.pdf as of 2 January 2007).

Busch, Nathan, "China's Fissile Material Protection, Control, and Accounting: The Case for Renewed Collaboration," *Nonproliferation Review* 9, no. 3 (Fall-Winter 2002; available at http://cns.miis.edu/pubs/npr/vol09/93/93busch.pdf as of 1 August 2005).

----------, *No End in Sight: The Continuing Menace of Nuclear Proliferation* (Lexington, KY: University Press of Kentucky, 2004).

Bush, President George W., "President Delivers 'State of the Union'" (Washington, D.C.: The White House, Office of the Press Secretary, 28 January 2003; available at http://www.whitehouse.gov/news/releases/2003/01/20030128-19.html as of 30 December 2006).

----------, "President Speaks on War Effort to Citadel Cadets: Remarks by the President at the Citadel" (Washington, D.C.: The White House, Office of the Press Secretary, 11 December 2001; available at http://www.whitehouse.gov/news/releases/2001/12/20011211-6.html as of 5 March 2006).

Cameron, Gavin, "Multitrack Microproliferation: Lessons from Aum Shinrikyo and Al Qaeda," *Studies in Conflict and Terrorism* 22, no. 4 (October-December 1999).

----------, *Nuclear Terrorism: A Threat Assessment for the 21st Century* (New York: St. Martins Press, 1999).

Campbell, Kurt M., Ashton B. Carter, Steven E. Miller, and Charles A. Zraket, *Soviet Nuclear Fission: Control of the Nuclear Arsenal in a Disintegrating Soviet Union* (Cambridge, MA: Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 1991).

Carter, Ashton B., William J. Perry, and John M. Shalikashvili, "A Scary Thought: Loose Nukes in North Korea," *Wall Street Journal*, 6 February 2003.

Center for Nonproliferation Studies, Monterey Institute for International Studies, "Thieves of Nuclear Plant Equipment Arrested in Ukraine," *NIS Export Control Observer* (May 2004; available at http://cns.miis.edu/pubs/nisexcon/pdfs/ob_0405e.pdf as of 5 March 2005).

Chazan, Guy, "Chechens Turn on Each Other -- after Years of Attacking Russians, Local `Collaborators' Are New Foe," *Wall Street Journal*, 30 December 2002.

Chuen, Christina, "Chechnya Has Become a Danger to Us All: A Conduit for Loose Nukes," *International Herald Tribune*, 26 June 2004.

Chyba, Christopher F., Hal Feiveson, and Frank Von Hippel, *Preventing Nuclear Proliferation and Terrorism: Essential Steps to Reduce the Availability of Nuclear-Explosive Materials* (Palo Alto, Cal.: Center for International Security and Cooperation, Stanford Institute for International Studies, Stanford University and Program on Science and Global Security, Woodrow Wilson School of Public and International Affairs, Princeton University, 2005; available at http://iis-db.stanford.edu/pubs/20855/Prvnt_Nuc_Prlf_and_Nuc_Trror_2005-0407.pdf as of 2 January 2007).

Cirincione, Joseph, Jon B. Wolfsthal, and Miriam Rajkumar, *Deadly Arsenals: Nuclear Biological, and Chemical Threats*, 2nd ed. (Washington, D.C.: Carnegie Endowment for International Peace, 2005).

----------, "Libya," in *Deadly Arsenals: Nuclear Biological, and Chemical Threats* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.carnegieendowment.org/pdf/npp/18-Libya.pdf as of 10 December 2006).

Clark, Andrew E., and Andrew J Oswald, "Satisfaction and Comparison Income," *Journal of Public Economics* 61, no. 3 (September 1996).

Clifford, Frank, "U.S. Drops Anti-Terrorist Tests at Nuclear Plants Security: Shrinking Budget Is Cited: Simulated Attacks Had Found Serious Lapses at Half of Nation's Reactors," *Los Angeles Times*, 3 November 1998.

Coates, C.W., B.L. Broadhead, A.M> Krichinsky, R. W. Leggett, M. B. Emmett, and J. B. Hines, "Radiation Effects on Personnel Performance Capability and a Summary of Dose Levels for Spent Research Reactor Fuels," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July* (Northbrook, Ill.: INMM, 2006).

Cochran, Thomas B., "Safety and Control of Nuclear Materials and Nuclear Weapons," paper presented at Economic and Social Development in the Former Soviet Union and the Problem of Nuclear Disarmament, Como, Italy, 3-4 July 1995.

Cochran, Thomas B., William M. Arkin, and Milton M. Hoenig, *Nuclear Weapons Databook: Volume I: U.S. Nuclear Forces and Capabilities* (Cambridge, Mass.: Ballinger, 1984).

Cochran, Thomas, and Christopher Paine, "The Amount of Plutonium and Highly-Enriched Uranium Needed for Pure Fission Nuclear Weapons" (Washington, D.C.: Natural Resources Defense Council, 13 April 1995; available at http://www.nrdc.org/nuclear/fissionw/fissionweapons.pdf as of 19 July 2005).

Cockburn, Andrew, and Leslie Cockburn, *One-Point Safe* (New York: Anchor Books/Doubleday, 1997).

Cockburn, Patrick, "America Quietly Sacks Its Prize Witness against Saddam," *Independent*, 17 April 2004 (available at http://www.commondreams.org/headlines04/0417-12.htm as of 10 December 2006).

Coll, Steve, "What Bin Laden Sees in Hiroshima," *Washington Post*, 6 February 2005.

Comella, Patricia A., "Revising the Convention on the Physical Protection of Nuclear Material--Chapter VI," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President* (Washington, D.C.: WMD Commission, 2005; available at http://www.wmd.gov/report/ as of 2 January 2007).

Committee on Indigenization of Programs to Prevent Leakage of Plutonium and Highly Enriched Uranium from Russian Facilities, Office for Central Europe and Eurasia, National Research Council, *Strengthening Long-Term Nuclear Security: Protecting Weapon-*

Usable Material in Russia (Washington, D.C.: National Academy Press, 2005; available at http://fermat.nap.edu/catalog/11377.html as of 4 April 2006).

Cornejo, Robert M., "When Sukarno Sought the Bomb: Indonesian Nuclear Aspirations in the Mid-1960s," *Nonproliferation Review* 7, no. 2 (Summer 2000; available at http://cns.miis.edu/pubs/npr/vol07/72/72corn.pdf as of 10 December 2006).

Cotter, Donald R., "Peacetime Operations: Safety and Security," in *Managing Nuclear Operations*, ed. Ashton B. Carter, Charles A. Zraket and John D. Steinbruner (Washington, D.C.: Brookings Institution, 1987).

Cullison, Alan, and Andrew Higgins, "Files Found: A Computer in Kabul Yields a Chilling Array of Al Qaeda Memos," *The Wall Street Journal*, 31 December 2001.

Curtis, Charles, "Promoting Global Best Practices," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005; available at http://www.nti.org/c_press/speech_curtisINMM_071105.pdf as of 8 June 2006).

Daly, Sara, John Parachini, and William Rosenau, *Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor: Implications of Three Case Studies for Combating Nuclear Terrorism* (Santa Monica, Cal.: RAND, 2005; available at http://www.rand.org/pubs/documented_briefings/2005/RAND_DB458.sum.pdf as of 5 January 2007).

Dan, Tang, "Physical Protection System and Vulnerability Analysis Program in China: Presentation to the Managing the Atom Seminar" (23 March 2004).

Dan, Tang, Yin Xiangdong, Fang Ni, and Guo Cao, "Physical Protection System and Vulnerability Analysis Program in China," in *Eu-High Level Scientific International Conference on Physical Protection* (Salzburg, Austria: Austrian Military Periodical, 2002; available at http://www.numat.at/list%20of%20papers/tangdan%20-%20unkorrigiert.pdf as of 5 April 2006).

Daniel Patrick Moynihan, chair, *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy*, Senate Document 105-2 (Washington, D.C.: Government Printing Office, 1997; available at http://www.fas.org/sgp/library/moynihan/ as of 18 August 2005).

Davis, Greg E., Lorilee Brownell, Troy Wright, John Tuttle, Mitchel Cunningham, and Patricia O'Brien, "Creating a Comprehensive, Efficient and Sustainable Nuclear Regulatory Structure: A Process Report from the U.S. Department of Energy's Material Protection, Control and Accounting Program," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).

Deich, Mark, "The Ingushetia Knot," *Moskovskii Komsomolets*, 6 August 2004.

Denton, Andrew, "Enough Rope (Interview with Hamid Mir)," *Australian Broadcasting Corporation*, 22 March 2004 (available at http://www.abc.net.au/tv/enoughrope/transcripts/s1071804.htm as of 5 January 2007).

Desmond, William J., Neil R. Zack, and James W. Tape, "The First Fifty Years: A Review of the Department of Energy Domestic Safeguards and Security Program," *Journal of Nuclear Materials Management* 26, no. 2 (Spring 1998).

Diakov, Anatoli, Eugene Miasnikov, and Timur Kadyshev, *Non-Strategic Nuclear Weapons: Problems of Control and Reduction* (Moscow: Center for Arms Control, Energy, and Environmental Studies, Moscow Institute of Physics and Technology, 2004; available at http://www.armscontrol.ru/pubs/en/NSNW_en_v1b.pdf as of 17 March 2005).

Director of Civil Nuclear Security, *The State of Security in the Civil Nuclear Industry and the Effectiveness of Security Regulation: April 2002 – March 2003* (London: Office for Civil Nuclear Security, Department of Trade and Industry, 2003; available at http://www.dti.gov.uk/files/file23303.pdf?pubpdfdload=03%2F418 as of 28 July 2006).

Dixon, Robyn, "Chechnya's Grimmest Industry: Thousands of People Have Been Abducted by the War-Torn Republic's Kidnapping Machine," *Los Angeles Times*, 18 September 2000.

Dodder, Rebecca S., Joseph M. Sussman, and Joshua B. McConnell, "The Concept of the 'CLIOS Process': Integrating the Study of Physical and Policy Systems Using Mexico City as an Example" (Cambridge, MA: Massachusetts Institute of Technology, Engineering Systems Division, 5 March 2004; available at http://esd.mit.edu/symposium/pdfs/papers/dodder.pdf as of 30 December 2006).

Duelfer, Charles, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at https://www.cia.gov/cia/reports/iraq_wmd_2004/index.html as of 10 December 2006).

----------, "Volume I: Regime Finance and Procurement," in *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at http://www.foia.cia.gov/duelfer/Iraqs_WMD_Vol1.pdf as of 10 December 2006).

----------, "Volume II: Nuclear," in *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (Langley, Vir.: U.S. Central Intelligence Agency, 2004; available at http://www.foia.cia.gov/duelfer/Iraqs_WMD_Vol2.pdf as of 10 December 2006).

Duffy, Robert J., *Nuclear Politics in America: A History and Theory of Government Regulation* (Lawrence, Kans.: University Press of Kansas, 1997).

Dunlop, William, and Harold Smith, "Who Did It? Using International Forensics to Detect and Deter Nuclear Terrorism," *Arms Control Today* 36, no. 8 (October 2006; available at http://www.armscontrol.org/act/2006_10/CVRForensics.asp as of 28 December 2006).

Dunn, Guy, *WMRC Global Terrorism Index 2003/2004* (London: World Markets Research Centre, 2003).

Edwards, John, and Jack Kemp, with Stephen Sestanovich, *Russia's Wrong Direction: What the United States Can and Should Do*, ed. Stephen Sestanovich, Independent Task Force Report No. 57 (New York: Council on Foreign Relations, 2006; available at http://www.cfr.org/content/publications/attachments/Russia_TaskForce.pdf as of 17 May 2006).

Einhorn, Robert J., and Gary Samore, "Ending Russian Assistance to Iran's Nuclear Bomb," *Survival* 44, no. 2 (May 2002).

Engineering, Institute of Physics and Power, "Third Russian International Conference on Nuclear Material Protection, Control, and Accounting," Obninsk, Russia, 16-20 May 2005.

Falkenrath, Richard A., Robert Newman, and Bradley Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, MA: MIT Press, 1998).

Feaver, Peter, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, N.Y.: Cornell University Press, 1992).

Feinstein, Lee, James C. Clad, Lewis A. Dunn, and David Albright, *A New Equation: U.S. Policy toward India and Pakistan after September 11* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.ceip.org/files/pdf/wp27.pdf as of 4 October 2006).

Ferguson, Charles, *Preventing Catastrophic Nuclear Terrorism* (Washington, D.C.: Council on Foreign Relations, 2006; available at http://www.cfr.org/content/publications/attachments/NucTerrCSR.pdf as of 8 June 2006).

Ferguson, Charles D., and William C. Potter, with Amy Sands, Leonard S. Spector and Fred L. Wehling, *The Four Faces of Nuclear Terrorism*, ed. Amy Sands, Leonard S. Spector and Fred L. Wehling (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004; available at http://www.nti.org/c_press/analysis_4faces.pdf as of 2 January 2007).

Ferguson, D.E., "Simple, Quick Reprocessing Plant" (Oak Ridge, Tenn.: Oak Ridge National Laboratory, 30 August 1977).

Fetter, Steve, Valery A. Frolov, Marvin Miller, Robert Mozley, Oleg F. Prilutsky, Stanislav N. Rodionov, and Roald Z. Sagdeev, "Detecting Nuclear Warheads," *Science and Global Security* 1 (1990; available at http://www.princeton.edu/~globsec/publications/pdf/1_3-4FetterB.pdf as of 13 August 2006).

Fetter, Steve, and Frank Von Hippel, "The Hazard from Plutonium Dispersal by Nuclear-Warhead Accidents," *Science and Global Security* 2, no. 1 (1990; available at http://www.princeton.edu/~globsec/publications/pdf/2_1Fetter.pdf as of 3 January 2006).

Fisher, Martin, "Income Is Development: Kickstart's Pumps Help Kenyan Farmers Transition to a Cash Economy," *Innovations* 1, no. 1 (Winter 2006; available at http://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2006.1.1.9 as of 29 December 2006).

Flores, Chris, "Project Sapphire: A Nuclear Odyssey: Defusing a Lethal Legacy," *News & Advance*, 29 December 2002.

Flory, Denis, "Revising the CPPNM: Challenges and Constraints," in *Proceedings of the 44th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 13-17 July 2003* (Northbrook, Ill.: INMM, 2003).

Forsberg, C. W., C. M. Hopper, J. L. Richter, and H.C. Vantine, *Definition of Weapons-Usable U-233*, ORNL/TM-13517 (Oak Ridge, Tenn.: Oak Ridge National Laboratory, 1998; available at http://www.ornl.gov/sci/criticality_shielding/HopperPubs/DefWeaponsUsableU-233ORNLTM13517.pdf as of 12 August 2006).

Frantz, Douglas, "A High-Risk Nuclear Stakeout: The U.S. Took Too Long to Act, Some Experts Say, Letting a Pakistani Scientist Sell Illicit Technology Well after It Knew of His Operation," *Los Angeles Times*, 27 February 2005.

Frost, Robin M., "Nuclear Terrorism after 9/11," *Adelphi Papers*, no. 378 (2005).

Garcia, Mary Lynn, *The Design and Evaluation of Physical Protection Systems* (Woburn, Mass.: Butterworth-Heineman, 2001).

Gardner, Byron, "Process of System Design and Analysis," paper presented at Workshop on Physical Protection, Moscow, 11-14 September 1995 (available at http://www.osti.gov/bridge/servlets/purl/112931-7hNczP/webviewable/112931.pdf as of 9 January 2007).

Garrick, B. John, "Perspectives on the Use of Risk Assessment to Address Terrorism," *Risk Analysis* 22, no. 3 (June 2002).

Gellman, Barton, and Dafna Linzer, "Unprecedented Peril Forces Tough Calls; President Faces a Multi-Front Battle against Threats Known, Unknown," *Washington Post*, 26 October 2004.

Gilinsky, Victor, Marvin Miller, and Harmon Hubbard, *A Fresh Examination of the Proliferation Dangers of Light Water Reactors* (Washington, D.C.: Nonproliferation Policy Education Center, 2004).

Gladwell, Malcolm, "Safety in the Skies: How Far Can Airline Security Go?" *The New Yorker* (1 October 2001; available at http://www.newyorker.com/fact/content/articles/011001fa_FACT as of 24 August 2005).

Glaser, Alexander, "On the Proliferation Potential of Uranium Fuel for Research Reactors at Various Enrichment Levels," *Science and Global Security* 14 (2006).

Glaser, Alexander, and Frank N. von Hippel, "Global Cleanout: Reducing the Threat of HEU-Fueled Nuclear Terrorism," *Arms Control Today* (January/February 2006; available at http://www.armscontrol.org/act/2006_01-02/JANFEB-heuFeature.asp as of 8 June 2006).

Glaser, Alexander, and Frank N. Von Hippel, "Thwarting Nuclear Terrorism," *Scientific American* 294, no. 2 (February 2006).

Goloskokov, Igor, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii (Reforming MVD Troops to Guard Russian Nuclear Facilities)," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9, no. 4 (Winter 2003; available at http://www.pircenter.org/data/publications/yk4-2003.pdf as of 28 February 2005).

Goodby, James E., Daniel L. Burghart, Cheryl A. Loeb, and Charles L. Thornton, *Cooperative Threat Reduction for a New Era* (Washington, D.C.: Center for Technology and National Security Policy, National Defense University, 2004; available at http://www.ndu.edu/ctnsp/CTR%20for%20a%20New%20Era.pdf as of 21 March 2005).

Gottemoeller, Rose, and Rebecca Longsworth, *Enhancing Nuclear Security in the Counter-Terrorism Struggle: India and Pakistan as a New Region for Cooperation* (Washington, D.C.: Carnegie Endowment for International Peace, 2002; available at http://www.ceip.org/files/pdf/wp29.pdf as of 21 March 2005).

Government of Canada, "Nuclear Safety and Control Act: Nuclear Security Regulations," *Canada Gazette Part II* 134, no. 13 (21 June 2000; available at http://canadagazette.gc.ca/partII/2000/20000621/pdf/g2-13413.pdf as of 20 November 2006).

----------, "Nuclear Safety and Control Act: Regulations Amending the Nuclear Security Regulations," *Canada Gazette Part II -- Extra* 140, no. 4 (7 September 2006; available at http://canadagazette.gc.ca/partII/2006/20060907-x4/pdf/g2-140x4.pdf as of 20 November 2006).

Greenpeace International, "The Action in Chalon: Greenpeace Blocks Plutonium Traffic" (19 February 2003; available at http://www.greenpeace.fr/stop-plutonium/en/20030219_en.php3 as of 5 May 2006).

Grindle, Merilee S., ed., *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries* (Cambridge, Mass.: Harvard University Press, 1997).

Gunaratna, Rohan, *Inside Al Qaeda: Global Network of Terror* (New York: Berkley Books, 2003).

Halevi, Jonathan D., "Al-Qaeda's Intellectual Legacy: New Radical Islamic Thinking Justifying the Genocide of Infidels," *Jerusalem Viewpoints*, no. 508 (1 December 2003; available at http://www.jcpa.org/jl/vp508.htm as of 4 December 2006).

Halilov, Holbay, "Minimizing Security Risks in Uzbekistan," paper presented at Seminar on Strengthening Nuclear Security in Asian Countries, Tokyo, 8-9 November 2006.

Hanan, N. A., M.M. Bretscher, A.P. Olson, and J. E. Matos, "Feasibility Studies for LEU Conversion of the Wwr-SM Reactor in Uzbekistan Using Pin-Type and Tubular Fuels,"

in *Proceedings of the 25th International Meeting on Reduced Enrichment for Research and Test Reactors, Chicago, Ill., 5-10 October 2003* (Argonne, Ill.: Argonne National Laboratory, 2003; available at http://www.rertr.anl.gov/RERTR25/PDF/Hanan.pdf as of 22 November 2006).

Handler, Joshua, *Russian Nuclear Warhead Dismantlement Rates and Storage Site Capacity: Implications for the Implementation of START II and De-Alerting Initiatives*, AC-99-01 (Princeton, N.J.: Center for Energy and Environmental Studies, Princeton University, 1999).

Hannah, Roger, "Dounreay Security Has Been Dodgy for Years," *Scottish Daily Record*, 28 April 1998.

Harrington, Kevin J., *Physical Protection of Nuclear Material: National Comparisons* (Livermore, Cal.: Sandia National Laboratories in cooperation with Stanford University, Center for International Security and Cooperation, 1999).

Harrison, Selig, "Inside North Korea: Leaders Open to Ending Nuclear Crisis," *Financial Times*, 4 May 2004 (available at http://ciponline.org/asia/inside.htm as of 17 December 2006).

Hegland, Corine, and Gregg Webb, "The Threat," *National Journal* 37, no. 16 (15 April 2005; available at http://nationaljournal.com/about/njweekly/stories/2005/0415nj1.htm as of 30 December 2006).

Hersh, Seymour, *The Samson Option: Israel's Nuclear Arsenal and American Foreign Policy* (New York: Random House, 1991).

Higgins, Andrew, Guy Chazan, and Gregory L. White, "Battlefield Conversion: How Russia's Chechen Quagmire Became Front for Radical Islam," *Wall Street Journal*, 16 September 2004.

Hinton, J.P., R.W. Barnard, D.E. Bennett, R.W. Crocker, M.J. Davis, G.A. Harms, L.W. Kruse, J.A. Milloy, W.A. Swansiger, K.J. Ystesund, H.J. Groh, E.A. Hakkila, W.L. Hawkins, and E.E. Hill, *Proliferation Vulnerability Red Team Report*, SAND97-8203 (Albuquerque, N.M.: Sandia National Laboratories, 1996; available at http://www.osti.gov/bridge/servlets/purl/437625-gCUCGr/webviewable/437625.pdf as of 14 August October 2006).

Hippel, Frank von, and Edwin Lyman, "Appendix: Probabilities of Different Yields," *Science and Global Security* 4 (1993; available at http://www.princeton.edu/%7Eglobsec/publications/pdf/4_1Mark.pdf as of 5 December 2006).

Hirsch, Daniel, "The NRC: What, Me Worry?" *Bulletin of the Atomic Scientists* 58, no. 1 (January/February 2002; available at http://www.thebulletin.org/article.php?art_ofn=jf02hirsch as of 8 January 2007), pp. 38-44.

Hirsch, Daniel, David Lochbaum, and Edwin Lyman, "The Nrc's Dirty Little Secret," *Bulletin of the Atomic Scientists* (May/June 2003; available at http://www.thebulletin.org/article.php?art_ofn=mj03hirsch as of 5 February 2006), pp. 44-51.

Hoddeson, Lillian, Paul W. Henriksen, Roger A. Meade, and Catherine Westfall, *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945* (Cambridge, UK: Cambridge University Press, 1993).

Hoffman, Bruce, *Al Qaeda,Trends in Terrorism and Future Potentialities: An Assessment*, P-8078 (Santa Monica, Cal.: RAND, 2003; available at http://www.rand.org/pubs/papers/P8078/P8078.pdf as of 4 April 2006).

----------, *Does Our Counter-Terrorism Strategy Match the Threat?* CT-250-1 (Santa Monica, Calif.: RAND, 2005; available at http://www.rand.org/pubs/testimonies/2005/RAND_CT250-1.pdf as of 28 December 2006).

----------, *Inside Terrorism* (New York: Columbia University Press, 2006).

----------, "Terrorism and WMD: Some Preliminary Hypotheses," *Nonproliferation Review* 4, no. 3 (1997; available at http://cns.miis.edu/pubs/npr/vol04/43/hoffma43.pdf as of 2 January 2007).

Hoffman, Bruce, Christina Meyer, Benjamin Schwarz, and Jennifer Duncan, *Insider Crime: The Threat to Nuclear Facilities and Programs*, R-3782-DOE (Santa Monica, Cal.: RAND, 1990).

Holdren, John P., and Matthew Bunn, "Technical Background: A Tutorial on Nuclear Weapons and Nuclear-Explosive Materials," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/cnwm/overview/technical.asp as of 16 February 2006).

Holgate, Laura, "Accelerating the Blend-Down of Russian Highly Enriched Uranium," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005; available at http://www.nti.org/c_press/analysis_Holgate_INMM%20Paper_061005.pdf as of 28 December 2006).

Hynes, Michael V., John E. Peters, and Joel Kvitky, "Denying Armageddon," *Annals of the American Academy of Political and Social Science* 607 (September 2006).

International Atomic Energy Agency, *Annual Report 2004* (Vienna: IAEA, 2005; available at http://www.iaea.org/Publications/Reports/Anrep2004/anrep2004_full.pdf as of 3 January 2007).

----------, "Calculating the New Global Nuclear Terrorism Threat" (Vienna: IAEA, 1 November 2001; available at http://www.iaea.org/NewsCenter/PressReleases/2001/nt_pressrelease.shtml as of 16 September 2005).

----------, *Communication Received from Japan Concerning Its Policies Regarding the Management of Plutonium*, INFCIRC/549/Add.1/9 (Vienna: IAEA, 2006; available at http://www.iaea.org/Publications/Documents/Infcircs/2006/infcirc549a1-9.pdf as of 21 November 2006).

----------, *Communication Received from the France Concerning Its Policies Regarding the Management of Plutonium*, INFCIRC/549/Add. 5/9 (Vienna: IAEA, 2005; available at http://www.iaea.org/Publications/Documents/Infcircs/2005/infcirc549a5-9.pdf as of 16 May 2006).

----------, *Communication Received from the United Kingdom of Great Britain and Northern Ireland Concerning Its Policies Regarding the Management of Plutonium*, INFCIRC/549/Add. 8/8 (Vienna: IAEA, 2006; available at http://www.iaea.org/Publications/Documents/Infcircs/2006/infcirc549a8-8.pdf as of 16 May 2006).

----------, *Communications Received from Certain Member States Regarding Guidelines for the Export of Nuclear Material, Equipment and Technology*, INFCIRC/254/Rev. 7/Part 1 (Vienna: IAEA, 2005; available at http://www.nuclearsuppliersgroup.org/PDF/infcirc254r7p1-050223.pdf as of 20 July 2005).

----------, *The Convention on Physical Protection of Nuclear Material*, INFCIRC/274/Rev. 1 (Vienna: IAEA, 1980; available at http://www.iaea.org/Publications/Documents/Infcircs/Others/inf274r1.shtml as of 29 July 2005).

----------, *Convention on the Physical Protection of Nuclear Material*, Legal Series No. 12 (Vienna: IAEA, 1982).

----------, "Convention on the Physical Protection of Nuclear Material" (Vienna: IAEA, December 2006; available at http://www.iaea.org/Publications/Documents/Conventions/cppnm_status.pdf as of 5 January 2007).

----------, *Fourth Consolidated Report of the Director General of the International Atomic Energy Agency under Paragraph 16 of Security Council Resolution 1051 (1996)*, S/1997/779 (New York: United Nations, 1997; available at http://www.iaea.org/worldatom/Programmes/ActionTeam/reports/s_1997_779.pdf as of 10 December 2006).

----------, "IAEA Regional Training Course on Security for Nuclear Installations," Mumbai, India, 11-20 May 2003.

----------, *IAEA Safeguards Glossary* (Vienna: IAEA, 2001; available at http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/Start.pdf as of 19 July 2005).

----------, *Illicit Trafficking and Other Unauthorized Activities Involving Nuclear and Radioactive Materials* (Vienna: IAEA, 2006; available at

http://www.iaea.org/NewsCenter/Features/RadSources/PDF/fact_figures2005.pdf as of 29 January 2007).

----------, *Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran*, GOV/2004/83 (Vienna: IAEA, 2004; available at http://www.iaea.org/Publications/Documents/Board/2004/gov2004-83.pdf as of 18 December 2006).

----------, "In Focus: IAEA and Iran" (Vienna: IAEA, 2006; available at http://www.iaea.org/NewsCenter/Focus/IaeaIran/index.shtml as of 5 May 2006).

----------, *Measures to Improve the Security of Nuclear Materials and Other Radioactive Materials*, GC(45)/INF/14 (Vienna: IAEA, 2001; available at http://www.iaea.org/About/Policy/GC/GC45/Documents/gc45inf-14.pdf as of 9 May 2006).

----------, "New Life for Research Reactors? Bright Future but Far Fewer Projected" (Vienna: IAEA, 8 March 2004; available at http://www.iaea.org/NewsCenter/Features/ResearchReactors/reactors20040308.html as of 5 January 2007).

----------, *Nuclear Security - Measures to Protect against Nuclear Terrorism: Amendment to the Convention on the Physical Protection of Nuclear Material*, GOV/INF/2005/10-GC(49)/INF/6 (Vienna: IAEA, 2005; available at http://www.iaea.org/About/Policy/GC/GC49/Documents/gc49inf-6.pdf as of 9 May 2006).

----------, *The Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.4 (Corrected) (Vienna: IAEA, 1999; available at http://www.iaea.or.at/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4_content.html as of 22 December 2006).

----------, ed., *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations, Vienna, 10-14 November* (Vienna: IAEA, 1997).

----------, *Proceedings of the Symposium on International Safeguards: Verification and Nuclear Material Security, Vienna, 29 October-2 November 2001* (Vienna: IAEA, 2001).

----------, *Safeguards Statement for 2005* (Vienna: IAEA, 2006; available at http://www.iaea.org/OurWork/SV/Safeguards/es2005.pdf as of 12 August 2006).

----------, *Security of Material: Measures to Prevent, Intercept, and Respond to Illicit Uses of Nuclear Material and Radioactive Sources: Proceedings of a Conference in Stockholm, Sweden, 7-11 May 2001* (Vienna: IAEA, 2001).

----------, *Sixth Consolidated Report of the Director General of the International Atomic Energy Agency under Paragraph 16 of UNSC Resolution 1051 (1996)* (New York: United Nations, 1998; available at http://www.nci.org/i/iaea10-8-98.htm as of 11 December 2006).

----------, "States Agree on Stronger Physical Protection Regime" (Vienna: IAEA, 8 July 2005; available at http://www.iaea.org/NewsCenter/PressReleases/2005/prn200503.html as of 22 August 2005).

----------, *Thorium Fuel Cycle -- Potential Benefits and Challenges*, TECDOC-1460 (Vienna: IAEA, 2005; available at http://www-pub.iaea.org/MTCD/publications/PDF/TE_1450_web.pdf as of 12 August 2006).

International Panel on Fissile Materials, *Global Fissile Material 2006: Report of the International Panel on Fissile Materials* (Princeton, N.J.: Program on Science and Global Security, Princeton University, 2006; available at http://www.fissilematerials.org/ipfm/site_down/ipfmreport06.pdf as of 24 January 2007).

Ivanov, Sergei, "Remarks to the Center for Defense Information" (Washington, D.C.: CDI, 6 April 2004).

Jameson, Angela, "Elite Armed Force Stands Firm after Nuclear Shake-Up: The Saturday Interview: Bill Pryke," *The Times*, 14 August 2004.

Jenkins, Bonnie, "Establishing International Standards for Physical Protection of Nuclear Material," *Nonproliferation Review* 5, no. 3 (Spring-Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/jenkin53.pdf as of 19 July 2005).

Jenkins, Brian M., "Will Terrorists Go Nuclear? A Reappraisal," in *The Future of Terrorism: Violence in the New Millenium*, ed. Harvey W. Kushner (London: Sage, 1998).

Jenkins, Brian Michael, and Joseph L. Krofcheck, "Appendix III-A: The Potential Nuclear Non-State Adversary," in *Nuclear Proliferation and Safeguards* (Washington, D.C.: Office of Technology Assessment, 1977).

Johnston, William Robert, "Nuclear Terrorism Incidents" (28 September 2003; available at http://www.johnstonsarchive.net/nuclear/wrjp1855.html as of 5 January 2007).

Jones, Rodney W., and Mark G. McDonough, *Tracking Nuclear Proliferation: A Guide in Maps and Charts* (Washington D.C: Carnegie Endowment for International Peace, 1998; available at http://www.ceip.org/programs/npp/track98b.htm as of 10 December 2006).

Kamp, Karl-Heinz, "Nuclear Terrorism Is Not the Core Problem," *Survival* 40, no. 4 (Winter 1998).

Kang, Jungmin, and Frank Von Hippel, "Limited Proliferation-Resistance Benefits from Recycling Unseparated Transuranics and Lanthanides from Light-Water Reactor Spent Fuel," *Science and Global Security* 13, no. 3 (2005).

Kang, Jungmin, and Frank N. von Hippel, "U-232 and the Proliferation-Resistance of U-233 in Spent Fuel," *Science and Global Security* 9 (2001; available at http://www.princeton.edu/~globsec/publications/pdf/9_1kang.pdf as of 12 August 2006).

Kaplan, David E., "Aum Shinrikyo," in *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, ed. Jonathan B. Tucker, Bcsia Studies in International Security (Cambridge, Mass.: MIT Press, 2000).

Kaplan, David E., and Andrew Marshall, *The Cult at the End of the World: The Terrifying Story of the Aum Doomsday Cult, from the Subways of Tokyo to the Nuclear Arsenals of Russia*, 1st American ed. (New York: Crown Publishers, 1996).

Kaufmann, Daniel, Aart Kraay, and Massimo Mastruzzi, *Governance Matters IV: Governance Indicators for 1996-2004* (Washington, D.C.: World Bank, 2005; available at http://www.worldbank.org/wbi/governance/pdf/GovMatters_IV_main.pdf as of 1 August 2006).

Kawai, H., H. Kurihara, and M. Kajiyoshi, "Physical Protection of Nuclear Material in Japan," in *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations: Proceedings of an International Conference, Vienna, 10-14 November 1997* (Vienna: International Atomic Energy Agency, 1997).

Keim, Paul, Kimothy L. Smith, Christine Keys, Hiroshi Takahashi, Takeshi Kurata, and Arnold Kaufmann, "Molecular Investigation of the Aum Shinrikyo Anthrax Release in Kameido, Japan," *Journal of Clinical Microbiology* 39, no. 12 (December 2001; available at http://www.pubmedcentral.nih.gov/articlerender.fcgi?tool=pubmed&pubmedid=11724885 as of 2 June 2005).

Kellen, Konrad, "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists," in *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Cambridge, Mass.: Lexington Books for the Nuclear Control Institute, 1987).

Khan, Afzal, "Pakistan's Hunt for Al Qaeda in South Waziristan," *The Jamestown Foundation*, 22 April 2004 (available at http://www.jamestown.org/news_details.php?news_id=45 as of 5 December 2005).

Khan, Kamran, "Pakistan Releases Nuclear Scientists for Ramadan's End," *The Washington Post*, 16 December 2001.

Khan, Kamran, and Molly Moore, "2 Nuclear Experts Briefed Bin Laden, Pakistanis Say," *Washington Post*, 12 December 2001.

Khinshteyn, Aleksandr, "Secret Materials," trans. BBC Monitoring Service, "Russian Central TV," 29 November 2002.

Khripunov, Igor, and James Holmes, eds., *Nuclear Security Culture: The Case of Russia* (Athens, Georgia: Center for International Trade and Security, The University of Georgia, 2004; available at http://www.uga.edu/cits/documents/pdf/Security%20Culture%20Report%2020041118.pdf as of 18 February 2005).

King, Dave, and Steve Smith, "Doomed Nuke Plant Dogged by Trouble," *Scottish Daily Record*, 5 June 1998.

Koelling, J.J., and E.W. Barts, *Special Nuclear Material Self-Protection Criteria Investigation: Phases I and II*, vol. LA-9213-MS, NUREG/CR-2492 (Washington, D.C.: U.S. Nuclear Regulatory Commission, 1982; available at http://www.sciencemadness.org/lanl1_a/lib-www/la-pubs/00307470.pdf as of 28 September 2005).

Kohen, Marshall D., and Joseph D. Rivers, "DOE's Involvement in Negotiations on the Question of Whether to Revise the Convention on the Physical Protection of Nuclear Material," in *Proceedings of the 42nd Annual Meeting of the Institute for Nuclear Materials Management, Indian Wells, Cal., 14-18 July 2001* (Northbrook, Ill.: INMM, 2001).

Koknar, Ali M., "The Trade in Materials for Weapons of Mass Destruction," *International Police Review* (March-April 1999), pp. 24-25.

Koryashkin, Pavel, "Russian Nuclear Ammunition Depots Well Protected – Official," *ITAR-TASS*, 25 October 2001.

Kotter, John P., *Leading Change*, First ed. (Boston, MA: Harvard Business School Press, 1996).

Kovchegin, Dmitry, "Approaches to Design Basis Threat in Russia in the Context of Significant Increase of Terrorist Activity," in *Proceedings of the 44th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 13-17 July 2003* (Northbrook, Ill.: INMM, 2003; available at http://bcsia.ksg.harvard.edu/publication.cfm?program=STPP&ctype=paper&item_id=398 as of 22 March 2005).

Krass, Allan S., Peter Boksma, Boelie Elzen, and Wim A. Smit, *Uranium Enrichment and Nuclear Weapon Proliferation* (London: Taylor & Francis for the Stockholm International Peace Research Institute, 1983).

Kristensen, Hans M., *U.S. Nuclear Weapons in Europe: A Review of Post-Cold War Policy, Force Levels, and War Planning* (Washington, D.C.: Natural Resources Defense Council, 2005; available at http://www.nrdc.org/nuclear/euro/euro.pdf as of 19 July 2005).

Kristof, Nicholas D., "An American Hiroshima," *New York Times*, 11 August 2004.

Kroft, Steve, "Anonymous Revealed: Michael Scheuer, Former CIA Osama Bin Laden Unit Leader, Discusses Early Intelligence and Opportunities to Kill Osama Bin Laden," "60 Minutes," *CBS News*, 14 November 2004.

Kunreuther, Howard, and Geoffrey Heal, "Interdependent Security," *Journal of Risk and Uncertainty* 26, no. 2-3 (2003; available at http://opim.wharton.upenn.edu/risk/downloads/02-06-HK.pdf as of 5 February 2006).

Kupriyanova, Irina, "Assessing the Effectiveness of the U.S. Nuclear Material Accounting, Control, and Physical Protection Program in Russia," *Yaderny Kontrol* 7, no. 2 (March/April 2002).

Kurihara, Hiroyoshi, "The Protection of Fissile Materials in Japan," in *A Comparative Analysis of Approaches to the Protection of Fissile Materials: Proceedings of the Workshop at Stanford University, July 28-30, 1997* (Livermore, Cal.: Lawrence Livermore National Laboratory, 1997).

Lakdawalla, Darius, and George Zanjanji, *Insurance, Self-Protection, and Economics of Terrorism* (RAND Center for Terrorism and Risk Management Policy, 2004; available at http://www.rand.org/pubs/working_papers/2005/RAND_WR171.pdf as of 11 February 2006).

Lancaster, John, and Kamran Khan, "Pakistani Scientist Apologizes; Nuclear Assistance Unauthorized, He Says," *Washington Post*, 5 February 2004.

Landers, Christopher, "Reactors Identified for Conversion: Reduced Enrichment for Research and Test Reactors (RERTR) Program," in *RERTR 2005: 27th International Meeting on Reduced Enrichment for Research and Test Reactors, Boston, Mass., 6-10 November* (Argonne, Ill.: Argonne National Laboratory, 2005; available at http://www.rertr.anl.gov/RERTR27/PDF/S9-1_Landers.pdf as of 20 June 2006).

Langewiesche, William, "How to Get a Nuclear Bomb," *Atlantic Monthly* 298, no. 5 (December 2006), pp. 80-98.

Lawrence Livermore National Laboratory, *Comparative Analysis of Approaches to Protection of Fissile Materials: Proceedings of a Workshop at Stanford University, 28-30 July 1997* (Livermore, Cal.: LLNL, 1997).

Leachman, Robert B., and Phillip Althoff, *Preventing Nuclear Theft: Guidelines for Industry and Government* (New York: Praeger, 1972).

Lee, Rensselaer, *Nuclear Smuggling and International Terrorism: Issues and Options for U.S. Policy*, RL31539 (Washington, D.C.: Congressional Research Service, 2002).

----------, "Nuclear Smuggling: Patterns and Responses," *Parameters: U.S. Army War College Quarterly* (Spring 2003; available at http://carlisle-www.army.mil/usawc/Parameters/03spring/lee.pdf as of 5 December 2005).

Leeman, Sue, "Scotland Yard Foils Huge Jewel Heist," *Associated Press*, 8 November 2000.

Lehman, Stan, "In Brazil: Thieves Tunnel into Bank Vault for $67.8 Million," *Associated Press*, 10 August 2005.

Leventhal, Paul, "Testimony of Paul Leventhal on Behalf of the Nuclear Control Institute on the Recommendations of the NRC Safeguards Performance Assessment Task Force, to the Nuclear Regulatory Commission" (Washington, D.C.: Nuclear Control Institute, 5 May 1999).

Leventhal, Paul, and Yonah Alexander, *Preventing Nuclear Terrorism* (Lexington, MA: Lexington, 1987).

Levi, Michael, "Deterring Nuclear Terrorism," *Issues in Science and Technology* 20, no. 3 (2004; available at http://www.issues.org/20.3/levi.html as of 28 December 2006).

----------, *On Nuclear Terrorism* (Cambridge, Mass.: Harvard University Press, 2007).

Linkov, Igor, and Dmitriy Burmistrov, "Model Uncertainty and Choices Made by Modelers: Lessons Learned from the International Atomic Energy Agency Model Intercomparisons," *Risk Analysis* 23, no. 6 (2003).

Lugar, Richard G., *The Lugar Survey on Proliferation Threats and Responses* (Washington, D.C.: Office of Senator Lugar, 2005; available at http://lugar.senate.gov/reports/NPSurvey.pdf as of 2 January 2007).

Lugar, Richard, and Sam Nunn, "Connecting the Dots on Nuclear, Biological, and Chemical Terrorism: The Clear Danger and the Imperative of a Global Coalition Response" (Washington, D.C.: Nuclear Threat Initiative, 27 May 2002; available at http://www.nti.org/c_press/statement_nunnlugar_052702.pdf as of 22 December 2006).

Lumb, Ralph, *Report of the Advisory Panel on Safeguarding Special Nuclear Materials* (Washington, DC: Atomic Energy Commission, 1967).

Luongo, Kenneth N., and Isabelle Williams, "Seizing the Moment: Using the U.S.-Indian Nuclear Deal to Improve Fissile Material Security," *Arms Control Today* (May 2006; available at http://www.armscontrol.org/act/2006_05/usindiafissilesecurity.asp as of 12 May 2006).

Lyman, Edwin, and Alan Kuperman, "A Re-Evaluation of Physical Protection Standards for Irradiated HEU Fuel," in *The 24th International Meeting on Reduced Enrichment for Research and Test Reactors, Bariloche, Argentina, 5 November 2002* (Argonne, Ill.: Argonne National Laboratory, 2002; available at http://www.rertr.anl.gov/Web2002/index.html as of 16 May 2006).

Lyman, Edwin S., "Radiological Sabotage at Nuclear Power Plants: A Moving Target Set," in *Proceedings of the 41st Annual Meeting of the Institute for Nuclear Materials Management, New Orleans, Louisiana, 16-20 July 2000* (Northbrook, Ill.: INMM, 2000; available at http://www.nci.org/e/el-inmm2000.htm as of 18 August 2005).

----------, "Using Bilateral Mechanisms to Strengthen Physical Protection Worldwide," in *Proceedings of the 45th Annual Meeting of the Institute for Nuclear Materials Management, Orlando, Florida, 18-22-July* (Northbrook, Ill.: INMM, 2004; available at http://www.ucsusa.org/global_security/nuclear_terrorism/bilateral-mechanisms.html as of 21 November 2006).

MacKinnon, Mark, "Will Use Any Tactic, Chechen Warlord Warns," *Globe and Mail*, 2 November 2004.

Maerli, Morten Bremer, *Crude Nukes on the Loose? Preventing Nuclear Terrorism by Means of Optimum Nuclear Husbandry, Transparency, and Non-Intrusive Fissile Material Verification* (Oslo: Unipub AS, 2004; available at http://www.nupi.no/IPS/filestore/MBM_dissertation2004.pdf as of 4 April 2006).

Mansur, Michael, "Nuclear Plant Security Stirs Concern," *Kansas City Star*, 18 September 2001.

Mark, J. Carson, "Explosive Properties of Reactor-Grade Plutonium," *Science and Global Security* 4 (1993; available at http://www.princeton.edu/%7Eglobsec/publications/pdf/4_1Mark.pdf as of 9 January 2007).

Mark, J. Carson, Theodore B. Taylor, Eugene Eyster, William Maraman, and Jacob Wechsler, "Can Terrorists Build Nuclear Weapons?" in *Preventing Nuclear Terrorism*, ed. Paul Leventhal and Yonah Alexander (Lexington, Mass: Lexington Books, 1987; available at http://www.nci.org/k-m/makeab.htm as of 4 January 2006).

Marshall, Pearl, "U.K. Upgrading Nuclear Security by Posting Armed Police at Sites," *Nucleonics Week* (27 January 2005).

Martin, Joanne, *Organizational Culture: Mapping the Terrain*, First ed. (Thousand Oaks, CA: SAGE Publications, 2002).

Massing, Michael, "Now They Tell Us," *New York Review of Books* 51, no. 3 (26 February 2004; available at http://foi.missouri.edu/polinfoprop/nowtheytell.html as of 10 December 2006).

Masumitsu, Hiroshi, "Revised N-Law Inadequate to Cover All Terrorism Scenarios," *Daily Yomiuri*, 18 June 2005.

McCloud, Kimberly, and Matthew Osborne, "WMD Terrorism and Usama Bin Laden" (Monterey, Cal.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 20 November 2001; available at http://cns.miis.edu/pubs/reports/binladen.htm as of 5 April 2006).

McElheney, Victor K., "U.S. Adding to Safeguards in Tactical Nuclear Arms," *New York Times*, 18 December 1973.

McLeod, Ian, "Bombs Away: Forty-Five Kilograms of Bomb-Grade Uranium Are Stockpiled at Chalk River, Awaiting the Long-Delayed Startup of Two Nuclear Reactors," *Ottawa Citizen*, 17 June 2006.

----------, "How to Keep Nuclear Sites Safe: Stage Mock Terror Attacks: Chalk River Considers U.S.-Style Security Drill," *Ottawa Citizen*, 17 June 2006.

McPhee, John, *The Curve of Binding Energy: A Journey into the Awesome and Alarming World of Theodore B. Taylor* (New York, NY: Farrar, Strauss, & Giroux, 1974).

McSween, Terry E., *The Values-Based Safety Process: Improving Your Safety Culture with Behavior-Based Safety* (Hoboken, N.J.: Wiley-Interscience, 2003).

Meadows, Donella H, "Whole Earth Models and Systems," *CoEvolution Quarterly* (Summer 1982; available at http://www.oss.net/dynamaster/file_archive/040324/48c97c243f534eee32d379e69b039289/WER-INFO-73.pdf as of 15 August 2005), pp. 98-108.

Mendelsohn, Catherine, "Scope and Accomplishments of the NNSA Nuclear Material Threat Reduction Program," in *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 10-14 July 2005* (Northbrook, Ill.: INMM, 2005).

Mir, Hamid, "Osama Claims He Has Nukes: If US Uses N-Arms It Will Get Same Response," *Dawn*, 10 November 2001 (available at http://www.dawn.com/2001/11/10/top1.htm as of 5 January 2007).

Moltz, James Clay, "Special Report: Assessing U.S. Nonproliferation Assistance in the NIS," *Nonproliferation Review* 7, no. 1 (Spring 2000 2000; available at http://cns.miis.edu/pubs/npr/vol07/71toc.htm as of 4 December 2006).

Moore, Chris, "Anatomy of a £26.5 Million Heist," *Sunday Life*, 21 May 2006.

Nakata, H., T. Misaka, and H. Tsuruta, "Experience in the Implementation of Physical Protection Measures of Nuclear Material at the JAERI Tokai Establishment," in *Physical Protection of Nuclear Materials: Experience in Regulation, Implementation, and Operations: Proceedings of an International Conference, Vienna, 10-14 November 1997* (Vienna: International Atomic Energy Agency, 1997).

National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 1st ed. (New York: Norton, 2004; available at http://www.gpoaccess.gov/911/index.html as of 30 December 2006).

National Research Council, *Material Control and Accounting in the Department of Energy's Nuclear Fuel Complex* (Washington, DC: National Academy Press, 1989).

Negroponte, John D., "Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence" (Washington, D.C.: 2 February 2006; available at http://www.fas.org/irp/congress/2006_hr/020206negroponte.pdf as of 26 December 2006).

Nelan, Bruce W., "Present Danger: Russia's Nuclear Forces Are Sliding into Disrepair and Even Moscow Is Worried About What Might Happen," *Time Europe* 149, no. 14 (7 April 1997), p. 42.

Neuffer, Elizabeth, "Gardner: Masterwork of Crime: Retracing the Steps of Robbery's Twisted Trail," *Boston Globe*, 13 May 1990.

----------, "A US Concern: Pakistan's Arsenal: Anti-American Mood Poses a Security Risk," *Boston Globe* 2002.

Norris, Robert S., and Hans M. Kristensen, "NRDC Nuclear Notebook: Dismantling U.S. Nuclear Warheads," *Bulletin of the Atomic Scientists* 60, no. 1 (January/February 2004; available at http://www.thebulletin.org/article_nn.php?art_ofn=jf04norris as of 5 December 2005), pp. 72-74.

----------, "NRDC Nuclear Notebook: Russian Nuclear Forces, 2005," *Bulletin of the Atomic Scientists* 61, no. 2 (March/April 2005; available at http://www.thebulletin.org/article_nn.php?art_ofn=ma05norris as of 1 March 2005), pp. 70-72.

----------, "NRDC Nuclear Notebook: U.S. Nuclear Forces, 2005," *Bulletin of the Atomic Scientists* 61, no. 1 (January/February 2005; available at http://www.thebulletin.org/article_nn.php?art_ofn=jf05norris as of 8 January 2007), pp. 73-75.

Norris, Robert S., and Hans S. Kristensen, "NRDC Nuclear Notebook: Global Nuclear Stockpiles, 1945-2006," *Bulletin of the Atomic Scientists* 62, no. 4 (July/August 2006; available at http://www.thebulletin.org/article_nn.php?art_ofn=ja06norris as of 13 August 2006), pp. 64-66.

Norway, Government of, "Statement by Norway," in *48th IAEA General Conference, Vienna, Austria, 20-21 September 2004* (Vienna: International Atomic Energy Agency, 2004; available at http://www.iaea.org/About/Policy/GC/GC48/Statements/norway.pdf as of 10 May 2006).

Nuclear Energy Institute, "Fact Sheet: Nuclear Power Plant Security" (Washington, D.C.: NEI, March 2005; available at http://www.nei.org/index.asp?catnum=3&catid=48 as of 18 August 2005).

Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, *Safeguarding a Domestic Mixed Oxide Industry against a Hypothetical Subnational Threat*, NUREG-0414 (Washington, D.C.: NRC, 1978).

Olson, Kyle B., "Aum Shinrikyo: Once and Future Threat?" *Emerging Infectious Diseases* 5, no. 4 (July-August 1999; available at http://www.cdc.gov/ncidod/EID/vol5no4/pdf/olson.pdf as of 2 June 2005).

Orlov, Vladimir, and William C. Potter, "The Mystery of the Sunken Gyros," *Bulletin of the Atomic Scientists* 54, no. 6 (November/December 1998; available at http://cns.miis.edu/research/iraq/gyro/index.htm as of 10 December 2006), pp. 34-39.

Orttung, Robert, and Louise Shelley, *Linkages between Terrorist and Organized Crime Groups in Nuclear Smuggling: A Case Study of Chelyabinsk Oblast*, PONARS Policy Memo No. 392 (Washington, D.C.: 2005; available at http://www.csis.org/media/csis/pubs/pm_0392.pdf as of 12 April 2006).

Ostanin, Sergei, "Chechen Terrorists out to Lay Hands on Nuclear Arms -- Military," *ITAR-TASS*, 30 January 2003.

Panel on U.S.-FSU Cooperation to Protect, Control, and Account for Weapons-Usable Nuclear Materials, President's Committee of Advisors on Science and Technology, *Securing Weapons-Usable Nuclear Materials in the Former Soviet Union: Urgent Measures to Prevent Nuclear Proliferation (U)*. Secret/Noforn (Washington, D.C.: Office of Science and Technology Policy, 1995).

Pankov, Andrey, "S Atomnoy Elektrostantsii Vynesli Tri Dorogostoyashchikh Klapana (Three High-Priced Valves Carried Off from Nuclear Power Plant)," *Novyye Izvestiya*, October 2004.

Parachini, John V., and David E. Mosher, *Diversion of NBC Weapons Expertise from the FSU: Understanding an Evolving Problem* (Santa Monica, Cal.: RAND, 2005).

Parliamentary Office of Science and Technology, *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*, vol. Report 222 (London: POST, 2004; available at http://www.parliament.uk/documents/upload/POSTpr222.pdf as of 2 August 2005).

Paxton, H.C., and N.L. Pruvost, *Critical Dimensions of Systems Containing 235U, 239Pu, and 233U: 1986 Revision* (Los Alamos, N.M.: Los Alamos National Laboratory, 1987; available at http://www.fas.org/sgp/othergov/doe/lanl/lib-www/la-pubs/00209019.pdf as of 9 January 2007).

Pellaud, Bruno, "Proliferation Aspects of Plutonium Recycling," *Journal of Nuclear Materials Management* 31, no. 1 (Fall 2002; available at http://www.inmm.org/topics/contents/fall02issue/pellaud.pdf as of 4 August 2006).

Perkovich, George, Jessica T. Mathews, Joseph Cirincione, Rose Gottemoeller, and Jon B. Wolfsthal, *Universal Compliance: A Strategy for Nuclear Security* (Washington, D.C.: Carnegie Endowment for International Peace, 2005; available at http://www.carnegieendowment.org/files/UC2.FINAL3.pdf as of 21 March 2005).

Petro, James B., and David A. Relman, "Understanding Threats to Scientific Openness," *Science* 302, no. 5652 (12 December 2003).

Phillips, John Aristotle, and David Michaelis, *Mushroom: The Story of the a-Bomb Kid*, 1st ed. (New York: Morrow, 1978).

Pluta, Anna M., and Peter D. Zimmerman, "Nuclear Terrorism: A Disheartening Dissent," *Survival* 48, no. 2 (Summer 2006).

Pond, R.B., and J.E. Matos, *Nuclear Mass Inventory, Photon Dose Rate, and Thermal Decay Heat of Spent Research Reactor Fuel Assemblies (Rev. 1)*, ANL/RERTR/TM-26 (Argonne, Ill.: Argonne National Laboratory, 1996).

Potter, William C., "Before the Deluge? Assessing the Threat of Nuclear Leakage from the Post-Soviet States," *Arms Control Today* October (1995).

----------, "Project Sapphire: U.S.-Kazakhstani Cooperation for Nonproliferation," in John M. Shields and William C. Potter, (Cambridge, Ma: Mit Press, 1997)." in *Dismantling*

the Cold War: U.S. And NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program, ed. John M. Shields and William C. Potter (Cambridge, Mass.: MIT Press, 1997).

Potter, William, and Nikolai Sokov, "Practical Measures to Reduce the Risks Presented by Non-Strategic Nuclear Weapons," paper presented at The Weapons of Mass Destruction Commission, Stockholm2005 (available at http://www.wmdcommission.org/files/No8.pdf as of 18 April 2005).

Powell, Bill, Tim McGirk, Ghulam Hasnain, Sayed Talat Hussain, Timothy J. Burger, Elaine Shannon, Scott MacLeod, Andrew Purvis, Simon Robinson, and Nahid Siamdoust, "The Man Who Sold the Bomb," *Time* 165 (21 February 2005), p. 22.

President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington D.C.: PFIAB, 1999; available at http://www.fas.org/sgp/library/pfiab/ as of 13 December 2006).

Prindle, Nancy, "The U.S.-China Lab-to-Lab Technical Exchange Program," *Nonproliferation Review* 5, no. 3 (Summer 1998; available at http://cns.miis.edu/pubs/npr/vol05/53/prindl53.pdf as of 11 May 2006).

Project on Government Oversight, "Energy Ups Their DBT, NRC Still Making Excuses" (Washington, D.C.: POGO, 28 September 2004; available at http://pogoblog.typepad.com/pogo/2004/09/energy_ups_thei.html as of 5 December 2005).

----------, *Nuclear Power Plant Security: Voices from inside the Fences* (Washington D.C.: POGO, 2002; available at http://www.pogo.org/p/environment/eo-020901-nukepower.html as of 2 January 2007).

----------, *U.S. Nuclear Weapons Complex: Homeland Security Opportunities* (Washington, D.C.: POGO, 2005; available at http://pogo.org/p/homeland/ho-050301-consolidation.html as of 30 December 2006).

----------, *U.S. Nuclear Weapons Complex: Security at Risk* (Washington, D.C.: POGO, 2001; available at http://www.pogo.org/p/environment/eo-011003-nuclear.html as of 4 December 2006).

----------, *U.S. Nuclear Weapons Complex: Y-12 and Oak Ridge National Laboratory at High Risk* (Washington, D.C.: POGO, 2006; available at http://pogo.org/p/homeland/ho-061001-Y12.html as of 17 November 2006).

Ptchikin, Sergey, "Needles of Patriots: Attempts Made to Privatize Unique System for Protection against Terrorists," *Rossiskaya Gazeta*, 21 December 2004.

Reason, James, *Managing the Risks of Organizational Accidents* (Aldershot, U.K.: Ashgate, 1997).

Rees, Joseph V., *Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island* (Chicago: University of Chicago, 1996).

Reinstedt, Robert, and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, N-1498-SL (Santa Monica, Cal.: RAND, 1980).

Rempel, William C., and Douglas Frantz, "Global Nuclear Inquiry Stalls: Authorities Fear That the Extent of a Pakistani Scientist's Proliferation Ring Remains Unknown and That It Will Resume Work If Pressures Ease," *Los Angeles Times*, 5 December 2004.

Rhodes, Richard, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1986).

Richelson, Jeffrey T., "Defusing Nuclear Terror," *Bulletin of the Atomic Scientists* 58, no. 2 (March/April 2002; available at http://www.thebulletin.org/article.php?art_ofn=ma02richelson as of 28 December 2006), pp. 38-43.

Risen, James, and Steven Engelberg, "Signs of Change in Terror Goals Went Unheeded," *New York Times*, 14 October 2001.

Risen, James, and Judith Miller, "C.I.A. Tells Clinton an Iranian a-Bomb Can't Be Ruled Out," *New York Times*, 17 January 2000 (available at http://www.library.cornell.edu/colldev/mideast/iranbmba.htm as of 18 December 2006).

Ritchie, Iain, "IAEA Presentation on Threat Reduction Activities," paper presented at The Global Threat Reduction Initiative International Partners' Conference, Vienna, Austria, 18-19 September 2004.

Ritchie, Iain G., "Growing Dimensions: Spent Fuel Management at Research Reactors," *IAEA Bulletin* 40, no. 1 (March 1998; available at http://www.iaea.org/Publications/Magazines/Bulletin/Bull401/article7.html as of 20 September 2006).

Rivers, Joseph, and D.L. Whaley, "Review of the Department of Energy Graded Safeguards Table," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).

Robbins, Carla Anne, and Anne Cullison, "Closed Doors: In Russia, Securing Its Nuclear Arsenal Is an Uphill Battle," *The Wall Street Journal*, 26 September 2005.

Roberts, John B., II, "Nuclear Secrets and the Culture Wars," *American Spectator* 32, no. 5 (May 1999), pp. 34-39, 76.

Robinson, Philip, "Global Research Reactor Security Program," in *RERTR 2005: 27th International Meeting on Reduced Enrichment for Research and Test Reactors, Boston, Mass., 6-10 November* (Argonne, Ill.: Argonne National Laboratory, 2005).

Rodionov, Stanislav, "Could Terrorists Produce Low-Yield Nuclear Weapons?" in *High-Impact Terrorism: Proceedings of a Russian-American Workshop* (Washington, D.C.: National Academy Press, 2002).

Rohde, David, "General Denies Letting Secrets of a-Bomb out of Pakistan," *New York Times*, 27 January 2004.

Rosenberg, Eric, "Bin Laden after Nukes from Russia, CIA Expert Says," *Omaha World-Herald*, 21 November 2004.

Sageman, Marc, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

Samore, Gary, ed., *Iran's Strategic Weapons Programmes: A Net Assessment* (London: Taylor & Francis for the International Institute for Strategic Studies, 2005).

----------, ed., *Iraq's Weapons of Mass Destruction: A Net Assessment* (London: International Institute for Strategic Studies, 2002).

Saradzhyan, Simon, *Russia: Grasping Reality of Nuclear Terror* (Cambridge, Mass.: Belfer Center for Science and International Affairs, 2003; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/saradzhyan_2003_02.pdf as of 2 January 2007).

Saradzhyan, Simon, and Nabi Abdullaev, "Disrupting Escalation of Terror in Russia to Prevent Catastrophic Attacks," *Connections* (Spring 2005).

Schaper, Annette, "Nuclear Terrorism: Risk Analysis after 9/11," *Disarmament Forum*, no. 2 (2003; available at http://www.unidir.ch/pdf/articles/pdf-art1907.pdf as of 4 April 2006).

Schein, Edgar H., *The Corporate Culture Survival Guide* (San Francisco, CA: Jossey-Bass, 1999).

----------, *Organizational Culture and Leadership*, Third ed. (San Francisco, CA: Jossey-Bass, 2004).

Scheinman, Lawrence, "Transcending Sovereignty in the Management and Control of Nuclear Material," *IAEA Bulletin* 43, no. 4 (2001; available at http://www.iaea.org/Publications/Magazines/Bulletin/Bull434/article7.pdf as of 10 August 2005).

Serber, Robert, *The Los Alamos Primer: The First Lectures on How to Build an Atomic Bomb* (Berkeley: University of California Press, 1992).

Serebrennikov, Robert, "2002 Saw Several Thefts of Nuclear Materials, Isotope Products in Russia," *ITAR-TASS*, 5 March 2003.

Shelton, Thomas A., James M. Viebrock, Alexander W. Riedy, Stanley D. Moses, and Helen M. Bird, "Multilateral Nonproliferation Cooperation: US - Led Effort to Remove HEU/LEU Fresh and Spent Fuel

from the Republic of Georgia to Dounreay, Scotland (Auburn Endeavor/Project Olympus)," in *Proceedings of the 21st International Meeting on Reduced Enrichment for Research and Test Reactors (RERTR), Sao Paulo, Brazil, 18-23 October 1998* (Argonne, Ill.:

Argonne National Laboratory, 1998; available at http://www.rertr.anl.gov/Fuels98/SpentFuel/SThomas.pdf as of 2 December 2006).

Shields, John M., and William C. Potter, *Dismantling the Cold War: U.S. And NIS Perspectives on the Nunn-Lugar Cooperative Threat Reduction Program* (Cambridge, MA: MIT Press, 1997).

Smith, Harold P., Jr., "Consolidating Threat Reduction," *Arms Control Today* 33, no. 9 (November 2003; available at http://www.armscontrol.org/act/2003_11/Smith.asp as of 22 March 2005), p. 19.

Snell, Mark K., "Estimation of Probability of Adversary Mission Success," in *Proceedings of the 47th Annual Meeting of the Institute for Nuclear Materials Management, Nashville, Tenn., 16-20 July 2006* (Northbrook, Ill.: INMM, 2006).

Soo Hoo, Mark, " IAEA Activities for the Physical Protection of Nuclear Material and Facilities -- the Role and Importance of IPPAS Missions," in *Eurosafe 2002, Berlin, 4-5 November 2002* (Berlin: Forum for Nuclear Safety, 2002; available at http://www.eurosafe-forum.org/products/data/5/pe_253_24_1_euro2_5_7_iaea_phys_pro.pdf as of 11 May 2006).

Sprinzak, Ehud, "The Great Superterrorism Scare," *Foreign Policy* (Fall 1998; available at http://jya.com/superterror.htm as of 4 April 2006).

Stein, Peter, and Peter Feaver, *Assuring Control of Nuclear Weapons: The Evolution of Permissive Action Links*, Csia Occasional Paper, No. 2 (Cambridge, Mass.: Center for Science and International Affairs, Harvard University, 1987).

Steinhausler, Fritz, ed., *Proceedings of Strengthening Global Practices for Protecting Nuclear Material: Eu-High Level Scientific International Conference on Physical Protection, Salzburg, Austria, 8-13 September* (Salzburg, Austria: University of Salzburg, 2002; available at http://www.numat.at/list%20of%20papers/gesamtproceedings.pdf as of 4 December 2006).

Sterman, John, *Business Dynamics: Systems Thinking and Modeling for a Complex World* (Irwin: McGraw-Hill, 2000).

Stern, Jessica, *The Ultimate Terrorists* (Cambridge, Mass.: Harvard University Press, 1999).

Stober, Dan, "No Experience Necessary," *Bulletin of the Atomic Scientists* 59, no. 2 (2003; available at http://www.thebulletin.org/article.php?art_ofn=ma03stober as of 27 February 2006).

Sublette, Carey, "Section 8.0: The First Nuclear Weapons," in *Nuclear Weapons Frequently Asked Questions* (2001; available at http://nuclearweaponarchive.org/Nwfaq/Nfaq8.html as of 12 December 2006).

Subramanian, Nirupama, "Pakistan Accepted U.S. Help on N-Plants," *The Hindu*, 22 June 2006 (available at http://www.thehindu.com/2006/06/22/stories/2006062205201400.htm as of 28 July 2006).

Summers, Chris, "Hopes of Finding Diamond Haul Fade," *BBC News Online*, 14 February 2004 (available at http://news.bbc.co.uk/1/hi/world/europe/3364911.stm as of 22 December 2005).

Sussman, Joseph M., "Toward Engineering Systems as a Discipline" (Cambridge, MA: Massachusetts Institute of Technology, Engineering Systems Division, 6 September 2000; available at http://esd.mit.edu/wps/esd-wp-2000-01.pdf as of 30 December 2006).

Suzuki, Tatsujiro, "Implications of 09/11 Terrorism for Civilian Nuclear Industry and Its Response Strategy," paper presented at Japan Atomic Industrial Forum-Harvard University Nonproliferation Workshop, Cambridge, Mass., 30-31 January 2002.

Swardson, Anne, "Armored Car Driver Strike Shortchanges Parisians; Atms Empty While Merchants Are Flush," *Washington Post*, 16 May 2000.

Tagliabue, John, "Latest in a Series of Bold Breaks Frees 3 Inmates at French Jail," *New York Times*, 15 April 2003.

Talmadge, Caitlin, "Striking a Balance: The Lessons of U.S.-Russian Materials Security Cooperation," *Nonproliferation Review* 12, no. 1 (March 2005; available at http://cns.miis.edu/pubs/npr/vol12/121/121talmadge.pdf as of 2 November 2005).

Terekhov, Aleksey, and Yevgeniy Latyshev, "Russian Missile Officers to Petition US for Resettlement Aid," *Novye Izvestiya*, 14 February 2005.

The Royal Society, *Management of Separated Plutonium* (London: Royal Society, 1998; available at http://www.royalsoc.ac.uk/displaypagedoc.asp?id=18551 as of 17 December 2006).

Timm, Ronald E., *Security Assessment Report for Plutonium Transport in France* (Paris: Greenpeace International, 2005; available at http://greenpeace.datapps.com/stop-plutonium/en/TimmReportV5.pdf as of 6 December 2005).

Tkachenko, Yevgeniy, "FSB Agents Prevent Theft of Nuclear Materials," *ITAR-TASS*, 18 December 1998.

Transparency International, *Corruption Perceptions Index 2004* (Berlin: TI, 2004; available at http://www.transparency.org/content/download/1532/7971/file/media_pack_en.pdf as of 16 November 2006).

----------, *Report on the Transparency International Global Corruption Barometer 2004* (Berlin: TI, 2004; available at http://www.transparency.org/content/download/1558/8065/file/barometer_report_8_12_2004.pdf as of 13 December 2006).

True, Doug, David Leaver, Ed Fenstermacher, and John Gaertner, *Risk Characterization of the Potential Consequences of an Armed Terrorist Ground Attack on a U.S. Nuclear Power Plant* (Palo Alto, Cal.: Electric Power Research Institute, 2003; available

at http://www.nei.org/documents/EPRINuclearPlantConsequencesStudy20032.pdf as of 26 September 2005).

U.S Committee on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, National Research Council, and Russian Committee on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, Russian Academy of Sciences, *Strengthening U.S.-Russian Cooperation on Nuclear Nonproliferation* (Washington, D.C.: National Academy Press, 2005; available at http://fermat.nap.edu/catalog/11302.html as of 2 January 2007).

U.S. and Russian Committees on Strengthening U.S. and Russian Cooperative Nuclear Nonproliferation, U.S. National Academy of Sciences and Russian Academy of Sciences, *Strengthening U.S.-Russian Cooperation on Nuclear Nonproliferation: Recommendations for Action* (Washington, D.C.: National Academy Press, 2005; available at http://books.nap.edu/catalog/11302.html as of 15 November 2005).

U.S. Central Intelligence Agency, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January through 30 June 1999* (Langley, Vir.: CIA, 2000; available at https://www.cia.gov/cia/reports/721_reports/jan_jun1999.html as of 18 December 2006).

----------, *Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January through 30 June 2003* (Langley, Vir.: CIA, 2004; available at https://www.cia.gov/cia/reports/721_reports/jan_jun2003.htm as of 18 December 2006).

U.S. Congress, General Accounting Office, *Nuclear Nonproliferation: Security of Russia's Nuclear Material Improving; Further Enhancements Needed*, GAO-01-312 (Washington, D.C.: GAO, 2001; available at http://www.gao.gov/new.items/d01312.pdf as of 2 January 2007).

----------, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: GAO, 2003; available at http://www.gao.gov/new.items/d03752.pdf as of 15 August 2005).

----------, *Quick and Secret Construction of Plutonium Reprocessing Plants: A Way to Nuclear Weapons Proliferation?* EMD-78-104 (Washington, D.C.: GAO, 1978).

----------, *Status of Transparency Measures for U.S. Purchase of Russian Highly Enriched Uranium* (Washington, D.C.: GAO, 1999; available at http://www.gao.gov/archive/1999/rc99194.pdf as of 18 July 2005).

----------, *Weapons of Mass Destruction: Additional Russian Cooperation Needed to Facilitate U.S. Efforts to Improve Security at Russian Sites*, GAO-03-482 (Washington, D.C.: GAO, 2003; available at http://www.gao.gov/new.items/d03482.pdf as of 4 March 2005).

U.S. Congress, Government Accountability Office, *Nuclear Security: DOE Needs to Resolve Significant Issues before It Fully Meets the New Design Basis Threat* (GAO, 200423 December 2006).

U.S. Congress, Government Accountability Office, *Nuclear Nonproliferation: DOE Needs to Consider Options to Accelerate the Return of Weapons-Usable Uranium from Other Countries to the United States and Russia*, GAO-05-57 (Washington, D.C.: GAO, 2004; available at http://www.gao.gov/new.items/d0557.pdf as of 2 February 2005).

----------, *Nuclear Nonproliferation: DOE Needs to Take Action to Further Reduce the Use of Weapons-Usable Uranium in Civilian Research Reactors*, GAO-04-807 (Washington, D.C.: GAO, 2004; available at http://www.gao.gov/new.items/d04807.pdf as of 2 February 2005).

----------, *Nuclear Nonproliferation: IAEA Has Strengthened Its Safeguards and Nuclear Security Programs, but Weaknesses Need to Be Addressed*, GAO-06-93 (Washington, D.C.: GAO, 2005; available at http://www.gao.gov/new.items/d0693.pdf as of 10 May 2006).

----------, *Nuclear Security: Doe's Office of the Undersecretary for Energy, Science, and Environment Needs to Take Prompt, Coordinated Action to Meet the New Design Basis Threat* (Washington, D.C.: GAO, 2005; available at http://www.gao.gov/new.items/d05611.pdf as of 18 August 2005).

U.S. Congress, Office of Technology Assessment, *Nuclear Proliferation and Safeguards* (Washington, D.C.: OTA, 1977; available at http://www.wws.princeton.edu/ota/disk3/1977/7705/7705.PDF as of 12 December 2006).

U.S. Congress, Senate, Committee on Government Affairs, Permanent Subcommittee on Investigations, *Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo: Staff Statement* (Washington, D.C.: U.S. Government Printing Office, 1995; available at http://www.fas.org/irp/congress/1995_rpt/aum/index.html as of 5 January 2007).

U.S. Congress, General Accounting Office, *Combating Nuclear Terrorism: Federal Efforts to Respond to Nuclear and Radiological Threats and to Protect Emergency Response Capabilities Could Be Strengthened*, GAO-06-1015 (Washington, D.C.: GAO, 2006; available at http://www.gao.gov/new.items/d061015.pdf as of 20 November 2006).

U.S. Department of Defense, *Cooperative Threat Reduction Annual Report to Congress: Fiscal Year 2006* (Washington, D.C.: U.S. Department of Defense, 2005).

----------, *Proliferation: Threat and Response* (Washington, D.C.: DOD, 1997; available at http://www.defenselink.mil/pubs/prolif97/ as of 18 December 2006).

----------, *Proliferation: Threat and Response* (Washington, D.C.: DOD, 2001; available at http://www.defenselink.mil/pubs/ptr20010110.pdf as of 18 December 2006).

----------, "Section V: Nuclear Weapons Technology," in *Militarily Critical Technologies List* (Washington, D.C.: DOD, 1998; available at http://www.fas.org/irp/threat/mctl98-2/p2sec05.pdf as of 12 December 2005).

----------, *Summary of José Padilla's Activities with Al Qaeda* (Washington, D.C.: DOD, 2004; available at http://news.findlaw.com/nytimes/docs/padilla/pad52804dodsum5.html as of 2 January 2007).

U.S. Department of Energy, *2006 Strategic Plan: Office of International Material Protection and Cooperation, National Nuclear Security Administration* (Washington, D.C.: DOE, 2006).

----------, *Fiscal Year 2003 Budget Request: Detailed Budget Justifications—Weapons Safeguards and Security* (Washington, D.C.: DOE, 2002; available at http://www.cfo.doe.gov/budget/03budget/content/weapons/OthrWeap.pdf as of 4 August 2005).

----------, *FY 2006 Congressional Budget Request: National Nuclear Security Administration* (Washington, D.C.: DOE, 2005; available at http://www.cfo.doe.gov/budget/06budget/Content/Volumes/Vol_1_NNSA.pdf as of 18 July 2005).

----------, *FY 2006 Congressional Budget Request: National Nuclear Security Administration--Defense Nuclear Nonproliferation*, vol. 1, DOE/ME-0046 (Washington, D.C.: DOE, 2005; available at http://www.cfo.doe.gov/budget/06budget/Content/Volumes/Vol_1_NNSA.pdf as of 27 February 2006).

----------, *FY 2007 Congressional Budget Request: National Nuclear Security Administration--Defense Nuclear Nonproliferation*, vol. 1, DOE/CF-002 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_1_NNSA.pdf as of 3 January 2007).

----------, *FY 2007 Congressional Budget Request: Other Defense Activities*, vol. 2, DOE/CF-003 (Washington, D.C.: DOE, 2006; available at http://www.cfo.doe.gov/budget/07budget/Content/Volumes/Vol_2_ODA.pdf as of 22 December 2006).

----------, "GTRI: Two Successful Years of Reducing Nuclear Threats" (Washington, D.C.: DOE, May 2006; available at http://www.nnsa.doe.gov/docs/factsheets/2006/NA-06-FS04.pdf as of 21 June 2006).

----------, *Guide to Implementation of DOE 5633.3b, "Control and Accountability of Nuclear Materials"* (Washington, D.C.: DOE, 1995).

----------, *Highly Enriched Uranium: Striking a Balance (Revision 1)* (Washington, D.C.: DOE, 2001; available at http://www.fas.org/sgp/othergov/doe/heu/striking.pdf as of 23 May 2006).

----------, *Improving Nuclear Materials Security at the Institute of Nuclear Physics - Tashkent, Uzbekistan* (Washington, D.C.: DOE, 1996; available at http://www.nti.org/e_research/profiles/Uzbekistan/index_6084.html as of 2 June 2006).

----------, *Nuclear Material Control and Accountability*, DOE M 470.4-6 (Washington, D.C.: DOE, 2005).

----------, *Physical Protection*, DOE M 470.4-2 Chg. 1 (Washington, D.C.: DOE, 2006).

----------, *Plutonium: The First 50 Years: United States Plutonium Production, Acquisition, and Utilization from 1944 through 1994* (Washington, D.C.: DOE, 1996; available at http://www.fas.org/sgp/othergov/doe/pu50y.html as of 4 January 2007).

----------, *Restricted Data Declassification Decisions 1946 to the Present (RDD-7)* (Washington, D.C.: DOE, 2001; available at http://www.fas.org/sgp/othergov/doe/rdd-7.html as of 14 August 2006).

----------, "U.S. And Russia Agree to Strengthen Nuclear Material Protection" (Washington, D.C.: DOE, 29 November 2001; available at http://www.energy.gov/HQPress/releases01/novpr/pr01200_v.htm as of 9 January 2003).

U.S. Department of Energy, National Nuclear Security Administration, *Report to the United States Congress under Section 3132 of the FY 2005 Defense Authorization Act: Unclassified Executive Summary* (Washington, D.C.: DOE, 2006).

----------, "Secret Mission to Remove Highly Enriched Uranium Spent Nuclear Fuel from Uzbekistan Successfully Completed: Four Shipments Have Been Sent to a Secure Facility in Russia" (Washington, D.C.: NNSA, 27 September 2006; available at http://www.nnsa.doe.gov/docs/newsreleases/2006/PR_2006-04-20_NA-06-10.htm as of 16 May 2006).

----------, "Sensitive Nuclear Material out of Los Alamos TA-18 Facility" (Washington, D.C.: NNSA, 2 November 2005; available at http://www.nnsa.doe.gov/docs/newsreleases/2005/PR_2005-11-02_NA-05-27.pdf as of 26 December 2006).

----------, "U.S. And China Jointly Host Technology Exposition on Nuclear Material Security and International Safeguards: Collaborative Approaches to Enhancing Nuclear Material Security" (Washington, D.C.: NNSA, 24 October 2005; available at http://www.nnsa.doe.gov/na-20/docs/china_tech_demo.pdf as of 24 February 2006).

U.S. Department of Energy, Office of Arms Control and Nonproliferation, *Nonproliferation and Arms Control Assessment of Weapons-Usable Fissile Material Storage and Excess Plutonium Disposition Alternatives*, DOE/NN-0007 (Washington, D.C.: DOE, 1997; available at http://www.osti.gov/bridge/servlets/purl/425259-CXr7Qn/webviewable/425259.pdf as of 2 January 2007).

U.S. Department of Energy, Office of Security Affairs, Office of Safeguards and Security, *Manual for Protection and Control of Safeguards and Security Interests*, DOE-M-5632.1c-1 (Washington, D.C.: DOE, 1994; available at http://www.fas.org/irp/doddir/doe/m5632_1c-1/index.html as of 28 February 2006).

U.S. Department of Energy, Office of the Inspector General, *Audit Report: Recovery of Highly Enriched Uranium Provided to Foreign Countries*, DOE/IG-0638 (Washington, D.C.: DOE OIG, 2004; available at http://www.ig.doe.gov/pdf/ig-0638.pdf as of 3 March 2005).

U.S. Department of State, *Country Reports on Human Rights Practices: 2005* (Washington, D.C.: U.S. Department of State, 2006; available at http://www.state.gov/g/drl/rls/hrrpt/2005/ as of 22 November 2006).

----------, "Europe and Central Asia: Russia," in *International Narcotics Control Strategy Report: 2003* (Washington, D.C.: U.S. Department of State, 2004; available at http://www.state.gov/p/inl/rls/nrcrpt/2003/vol1/html/29838.htm as of 17 December 2006).

U.S. National Academy of Sciences, Committee on International Security and Arms Control, *Management and Disposition of Excess Weapons Plutonium* (Washington, D.C.: National Academy Press, 1994; available at http://books.nap.edu/html/plutonium/0309050421.pdf as of 30 December 2006).

----------, *Monitoring Nuclear Weapons and Nuclear-Explosive Materials* (Washington, D.C.: National Academy Press, 2005; available at http://books.nap.edu/catalog/11265.html as of 8 August 2005).

U.S. National Academy of Sciences, Panel on Reactor-Related Options, *Management and Disposition of Excess Weapons Plutonium: Reactor-Related Options* (Washington, D.C.: National Academy Press, 1995; available at http://books.nap.edu/html/plutonium/0309051452.pdf as of 30 December 2006).

U.S. National Academy of Sciences, Panel to Review the Spent Fuel Standard for Disposition of Excess Weapons Plutonium, *The Spent Fuel Standard for Disposition of Excess Weapons Plutonium: Application to Current DOE Options* (Washington, D.C.: National Academy Press, 2000; available at http://www.nap.edu/catalog/9999.html as of 15 August 2006).

U.S. National Intelligence Council, *Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces* (Washington, D.C.: Central Intelligence Agency, 2004; available at http://www.dni.gov/nic/special_russiannuke04.html as of 5 March 2005).

U.S. Nuclear Regulatory Commission, *In the Matter of Duke Energy Corporation (Catawba Nuclear Station, Units 1 and 2)*, CLI-04-29 (Washington, D.C.: NRC, 2004; available at http://www.nrc.gov/reading-rm/doc-collections/commission/orders/2004/2004-29cli.pdf as of 22 September 2006).

----------, *In the Matter of Duke Energy Corporation (Catawba Nuclear Station, Units 1 and 2)*, CLI-05-14 (Washington, D.C.: NRC, 2005; available at http://www.nrc.gov/reading-rm/doc-collections/commission/orders/2005/2005-14cli.html as of 22 Sepember 2006).

----------, *NRC Authorizes Use of Mixed Oxide Fuel Assemblies at Catawba Nuclear Power Plant* (Washington, D.C.: NRC, 2005; available at http://www.nrc.gov/reading-rm/doc-collections/news/2005/05-043.html as of 30 December 2006).

----------, "NRC Response to Letters to NRC Chairman Nils J. Diaz Regarding Security at Nuclear Power Plants" (Washington, D.C.: NRC, October 2004; available at http://www.nrc.gov/reading-rm/doc-collections/for-the-record/2004/nsir-response.pdf as of 18 August 2005).

----------, "Part 73-Physical Protection of Plants and Materials," in *Title 10, Code of Federal Regulations* (Washington, D.C.: U.S. Government Printing Office; available at http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html as of 28 September 2005).

U.S. Senate, Committee on Government Operations, *Peaceful Nuclear Exports and Weapons Proliferation: A Compendium* (Washington, D.C.: Government Printing Office, 1975).

U.S. Senate, Select Committee on Intelligence, *Report on the U.S. Intelligence Community's Prewar Assessments on Iraq* (2004; available at http://www.gpoaccess.gov/serialset/creports/iraq.html as of 11 December 2006).

United Nations, "1540 Committee" (New York: UN, 2005; available at http://disarmament2.un.org/Committee1540/meeting.html as of 25 February 2005).

United Nations, Office on Drugs and Crime, *Eighth United Nations Survey of Crime Trends and Operations of Criminal Justice Systems, Covering the Period 2001-2002* (New York: UN, 2005; available at http://www.unodc.org/unodc/en/crime_cicp_survey_eighth.html as of 16 November 2006).

USEC, "Chronology: U.S.-Russian Megatons to Megawatts Program: Recycling Nuclear Warheads into Electricity (as of October 1, 2006)" (Bethesda, Md.: USEC, October 2006; available at http://www.usec.com/v2001_02/HTML/Megatons_chronology.asp as of 3 January 2007).

Volodin, Yuri, Boris Kroupchatnikov, and Alexander Sanin, "MPC&A Regulatory Program in the Russian Federation: Trends and Prospective," in *Proceedings of the 43rd Annual Meeting of the Institute of Nuclear Materials Management, Orlando, Fla., 23-27 June 2002* (Northbrook, Ill.: INMM, 2002).

von Hippel, Frank, "A Comprehensive Approach to Elimination of Highly-Enriched Uranium from All Nuclear Reactor-Reactor Fuel Cycles," *Science and Global Security* 12, no. 3 (November 2004).

----------, "Fissile Material Security in the Post-Cold War World," *Physics Today* 48, no. 6 (June 1995).

Waas, Murray, "Intel Reports Cast Doubt on Iraq War Justifications," *Global Security Newswire*, 9 March 2006 (available at

http://www.nti.org/d_newswire/issues/2006/3/9/541C9625-EB23-4F5F-8A47-1663B968B897.html as of 13 March 2006).

Wadhams, Nick, "Center to Track Russian Nuclear Material," *Associated Press*, 4 November 1998.

Wald, Matthew L., "Battle Swirls on Security at a-Plants," *New York Times*, 6 August 2004 (available at http://pogo.org/m/hsp/hsp-nytimes-08062004.pdf as of 18 August 2005).

Walker, J. Samuel, "Regulating against Nuclear Terrorism: The Domestic Safeguards Issue, 1970-1979," *Technology and Culture* 42, no. 1 (January 2001).

Walsh, Jim, "Bombs Unbuilt: Power, Ideas, and Institutions in International Politics" (Ph.D. dissertation, Political Science, Massachusetts Institute of Technology, 2001).

Wampler, Stephen, "DOE Helps Chinese Agency to Secure Nuclear Material," *Lawrence Livermore National Laboratory's Weekly Newsline*, 16 December 2005 (available at http://www.llnl.gov/pao/employee/articles/2005/12.16.05.newsline.pdf as of 24 February 2006).

Weapons of Mass Destruction Terrorism Research Program, "Chart: Al Qa'ida's WMD Activities" (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 13 May 2005; available at http://cns.miis.edu/pubs/other/sjm_cht.htm as of 23 May 2006).

Wedekind, L., "Upgrading Nuclear Security Tops Board Agenda" (Vienna: International Atomic Energy Agency, 1 February 2002; available at http://www.iaea.org/NewsCenter/News/2002/01022002_news01.shtml as of 4 October 2005).

Weinzierl, Matthew C., "The Cost of Living: The Economics of Preventing Nuclear Terrorism," *The National Interest*, no. 75 (Spring 2004; available at http://www.findarticles.com/p/articles/mi_m2751/is_75/ai_n6076390/pg_1 as of 22 May 2006), pp. 118-122.

Whitlock, Craig, "Germany Arrests 2 Al Qaeda Suspects; Men Accused of Planning Attacks in Iraq," *Washington Post*, 24 January 2005.

Wier, Anthony, "Interdicting Nuclear Smuggling," in *Nuclear Threat Initiative Research Library: Securing the Bomb* (Cambridge, Mass., and Washington, D.C.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, 2002; available at http://www.nti.org/e_research/cnwm/interdicting/index.asp as of 1 March 2005).

Wight, Albert R., "Participation, Ownership, and Sustainable Development," in *Getting Good Government: Capacity Building in the Public Sectors of Developing Countries*, ed. Merilee S. Grindle (Cambridge, Mass.: Harvard University Press, 1997).

Willis, Henry H., Andrew R. Morral, Terrence K. Kelly, and Jamison Jo Medby, *Estimating Terrorism Risk* (Santa Monica, Cal.: RAND, 2005; available at http://www.rand.org/pubs/monographs/2005/RAND_MG388.pdf as of 6 May 2006).

Willrich, Mason, and Theodore B. Taylor, *Nuclear Theft: Risks and Safeguards* (Cambridge, MA: Ballinger, 1974).

Wilson, James Q., *Bureaucracy: What Government Agencies Do and Why They Do It*, 2nd ed. (New York: Basic Books, 2000).

Woo, Gordon, "Quantitative Terrorism Risk Assessment," *Journal of Risk Finance* 4, no. 1 (October 2002; available at http://www.rms.com/NewsPress/Quantitative_Terrorism_Risk_Assessment.pdf as of 22 May 2006).

World Bank, *Assessing Aid: What Works, What Doesn't, and Why* (Oxford, United Kingdom: Oxford University Press, 1998).

----------, *World Development Indicators: 2006* (Washington, D.C.: World Bank, 2006).

World Nuclear Association, "World Industry Lauds IAEA Initiative on Nuclear Safety and Security" (London: WNA, 2 November 2001).

Yamshanov, Boris, "Bribes Reeking of Explosives," *Rossiiskaya Gazeta*, 16 September 2004.

Yusufzai, Rahimullah, "Interview with Bin Laden: World's Most Wanted Terrorist" (ABC News, 1999; available at http://www.islamistwatch.org/blogger/localstories/05-06-03/ABCInterview.html as of 5 January 2007).

Zagorin, Adam, "Bordering on Nukes?" *Time* (22 November 2004), p. 19.

Zhang, Hui, "Evaluating China's MPC&A System," in *Proceedings of the 44th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., 13-17 July 2003* (Northbrook, Ill.: INMM, 2003; available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/MPC&A.pdf as of 1 August 2005).

Zimmerman, Peter D., and Jeffrey G. Lewis, "The Bomb in the Backyard," *Foreign Policy*, no. 157 (November/December 2006), pp. 32-39.