Nuclear Terrorism: How Big is the Risk to Japan?

Matthew Bunn

December 7, 2015

The meltdowns at the Fukushima Daichi nuclear power plant have appropriately focused Japan on the risks potentially posed by nuclear accidents. Japan has reformed its nuclear regulatory agency and focused intensely on improving nuclear safety.

But in addition to the risks of purely accidental events, the risks posed by *intentional* events – particularly terrorist actions – are also substantial, requiring further action to reduce them. Indeed, given the steps now being taken to prevent accidents, the risk that the next major release will occur as a result of terrorism may be as high as or higher than the risk that it will happen purely by accident. Hence, nuclear *security* is also critical – arguably, a facility cannot be said to be safe unless it is also secure.

This paper explores these risks, using a mathematical model of the risk of nuclear terrorism and accounts of the history of adversary actions against nuclear facilities to provide at least rough estimates of the magnitude of the risk. Finally, the paper offers recommendations for reducing nuclear theft and sabotage risks in Japan and around the world.[1]

Types of Nuclear and Radiological Terrorism

Three types of nuclear terrorism are each of concern:[2]

- ***Nuclear explosives.*** The most extreme and devastating form of nuclear terrorism is terrorist use of an actual nuclear bomb – either a stolen nuclear weapon or a crude bomb the terrorists managed to make themselves, from stolen plutonium or highly enriched uranium (HEU). This could turn the heart of a major city into a smoldering radioactive ruin, killing tens or hundreds of thousands of people and creating reverberating economic, military, and political consequences throughout the world. This would be the most technically challenging type of nuclear terrorist attack. The *probability* of such an event may not be high – though as discussed below, it is likely not as low as many think – but the *consequences* would be so immense that the overall *risk* remains high enough to justify immediate action to reduce it.

---

[1] This paper draws heavily on Matthew Bunn, Martin B. Malin, Nickolas Roth, and William H. Tobey, *Advancing Nuclear Security: Evaluating Progress and Setting New Goals* (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2014), http://belfercenter.hks.harvard.edu/files/advancingnuclearsecurity.pdf. It also draws in part on Matthew Bunn, *The Gates of Hell: Guarding Against Nuclear Theft and Terrorism* (Cambridge, Mass.: MIT Press, forthcoming).

[2] One prominent treatment of the topic divided the use of nuclear explosives into two possibilities – use of stolen nuclear weapons from a state, and use of improvised nuclear devices the terrorists made themselves – and hence divided the possibilities into four categories, rather than three. See Charles D. Ferguson and William C. Potter, with Amy Sands, Leonard S. Spector, and Fred L. Wehling, *The Four Faces of Nuclear Terrorism* (Monterey, Calif.: Center for Nonproliferation Studies, Monterey Institute of International Studies, 2004), http://www.nti.org/c_press/analysis_4faces.pdf.

- ***Nuclear sabotage.*** Another danger is the possibility of terrorist action to sabotage a major nuclear facility and cause a major radioactive release – a "terrorist Fukushima." As the Fukushima Daiichi accident showed, such an event could also widespread terror and huge economic consequences. Both the difficulty terrorists would face in accomplishing such an attack and the scale of the devastation they could cause by doing so are less than in the case of a nuclear explosives.
- ***"Dirty bombs."*** A radiological dispersal device, or "dirty bomb" simply takes radioactive material and spreads it over an area. This would be far easier for terrorists to accomplish than either of the other two types of nuclear terrorism, but far less devastating. In most cases, no one would be killed – though such a device could cause substantial panic, force the evacuation of multiple blocks of a major city, and impose many billions of dollars in disruption and cleanup costs.

Of course, in addition to these three categories, states also have to be prepared for a variety of potential threats and hoaxes – the most common form of terrorist activity related to nuclear or radiological material to date – but these are far less devastating than the actual use of radiological and nuclear materials.

This paper will focus primarily on nuclear explosives and nuclear sabotage, as it is these two that are intimately related to nuclear energy and its fuel cycle. The radiological material that might be used in a so-called "dirty bomb" exists in many thousands of facilities around the world, in virtually every country, for beneficial purposes ranging from medicine to industry, most of which have little to do with the nuclear industry. Security for such radiological sources is very important, but is largely beyond the scope of this paper.[3]

The Risk of Nuclear Terrorism: A Qualitative Approach

Nuclear theft and terrorism are not just hypothetical worries. There have been approximately 20 cases of seizure of stolen nuclear bomb material that are well documented in the public record, and multiple cases of actual or planned nuclear sabotage.[4]

Do terrorists want nuclear weapons? For most terrorists, focused on the limited violence appropriate for accomplishing local political objectives, the answer is no. But for a limited set of terrorists with extreme global objectives or apocalyptic visions, the answer is decidedly yes. Al Qaeda and the Japanese cult Aum Shinrikyo both made repeated attempts to get nuclear weapons or the material and expertise needed to make them, and there is evidence that Chechen terrorists may have sought nuclear weapons as well. Al Qaeda had a focused program reporting directly to Ayman al-Zawahiri, now the group's leader, which progressed as far as carrying out crude conventional explosive tests for the bomb program in the Afghan desert.[5] Most of the

---

[3] See, for example, the papers on the topic available at "Security for Radiological Sources," *Nuclear Security Matters*, http://nuclearsecuritymatters.belfercenter.org/security-radiological-sources.

[4] For the summary of the nuclear terrorism threat provided to the Sherpas for the 2014 nuclear security summit, see William H. Tobey and Pavel S. Zolotarev, "The Nuclear Terrorism Threat," Pattaya, Thailand, January 13, 2014, http://belfercenter.ksg.harvard.edu/files/nuclearterrorismthreatthailand2014.pdf.

[5] See, for example, Matthew Bunn, Yuri Morozov, Rolf Mowatt-Larssen, Simon Saradzhyan, William Tobey, Viktor I. Yesin, and Pavel S. Zolotarev, *The U.S.-Russia Joint Threat Assessment of Nuclear Terrorism* (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, and Institute for U.S. and Canadian Studies, 2011), http://belfercenter.ksg.harvard.edu/publication/21087/.

participants in al Qaeda's program – including the man who led it – have neither been killed nor captured.

There is no hard evidence in the public domain that the Islamic State (IS) is yet seeking nuclear weapons. But the Paris attacks make clear that they are planning mass casualty attacks far beyond their territory, and they have an apocalyptic ideology that envisions a final war between the "Crusader" forces and their Islamic forces, for which extremely powerful weapons would presumably be needed. If IS were to seek nuclear weapons, it has more money, more control of territory, more people, and more ability to recruit experts globally than al Qaeda at its best ever had – all of which could increase its chances of success.

Could terrorists make a crude nuclear bomb if they got the necessary nuclear material? Here, unfortunately, multiple studies by the U.S. government and other governments have concluded that the answer is "yes" – a sophisticated terrorist group with enough plutonium or HEU might well be able to fashion a crude but workable nuclear bomb.[6] As one U.S. government report summarized the issue in the 1970s, long before the voluminous information now available on the internet existed:[7]

> 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... Only modest machine-shop facilities that could be contracted for without arousing suspicion would be required.

This conclusion applied to both gun-type and implosion-type bombs. While an implosion bomb would be significantly more difficult for terrorists to build, it is not out of the question – particularly if they got knowledgeable help, as al Qaeda repeatedly attempted to do. A crude implosion device does not need to be as complex as the bomb that destroyed Nagasaki.

Nuclear material does not have to be "weapon-grade" to pose a serious danger that terrorists could use it to make a nuclear bomb. HEU at well below 90 percent U-235 could be used, at the price of using somewhat more material. The U.S. government has declassified the fact that any state or group that could make a bomb from weapons-grade plutonium could also make a bomb from reactor-grade plutonium. The "fizzle yield" – the explosive yield that would result if the extra neutrons from reactor-grade plutonium set off the chain reaction at the worst possible time – for a design similar to the Nagasaki bomb is in the range of a kiloton, and the probable yield is higher than that.[8] The heat from reactor-grade plutonium can also be managed by a variety of means: it should be remembered, for example, that early U.S. nuclear weapons were designed to have the plutonium core put into the bomb at the last moment, just before use.

Although the process of designing and building a crude nuclear bomb would probably be long and difficult, this may not always be the case. Indeed, for facilities with some types of material, U.S. Department of Energy (DOE) internal security regulations require that security

---

[6] Matthew Bunn and Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?" *Annals of the American Academy of Political and Social Science,* Vol. 607 (September 2006), pp. 133–149.

[7] U.S. Congress, Office of Technology Assessment, *Nuclear Proliferation and Safeguards* (Washington, D.C.: OTA, 1977), http://www.princeton.edu/~ota/disk3/1977/7705/7705.PDF, p. 140.

[8] 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), http://www.osti.gov/bridge/servlets/purl/425259-CXr7Qn/webviewable/425259.pdf, pp. 37-39.

plans 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 in the building*.[9]

What would the consequences of a nuclear terrorist attack be? In the city attacked, a huge area might be entirely destroyed, with tens or hundreds of thousands killed and hundreds of thousands more injured. Fires would likely rage out of control, far behind any plausible capability to fight them. With everything from roads to hospitals destroyed, organizing to provide food, water, shelter, and medical care to the survivors would be an immense challenge.10 The direct economic damage – measured in lives lost and property destroyed – might reach $1 trillion.[11]

Terrorists – either those who committed the attack or others – would probably claim they had more bombs already hidden in other cities (whether they did nor not), and the fear that this might be true could lead to panicked evacuations, creating widespread havoc and economic disruption. In what would inevitably be a desperate effort to prevent further attacks, traditional standards of civil liberties would likely be jettisoned, and the country attacked might well lash out militarily at whatever countries it thought might bear a portion of responsibility.[12] Far more than after the 9/11 attacks, international politics would be likely to become more brutish and

---

[9] 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), http://www.fas.org/irp/doddir/doe/m5632_1c-1/index.html. This order has now been superseded, 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, was expanded at DOE after the 9/11 attacks. 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* (Washington, D.C.: GAO, 2004), http://www.gao.gov/new.items/d04623.pdf.

[10] For a useful discussion of the need to prepare to respond to such an event – and the immense difficulty of doing so – see Ashton B. Carter, Michael M. May, and William J. Perry, *The Day After: Action in the 24 Hours Following a Nuclear Blast in an American City* (Cambridge, Mass.: Preventive Defense Project, Harvard and Stanford Universities, 2007), http://belfercenter.ksg.harvard.edu/publication/2140/.

[11] There have been many assessments of the impact of such an attack, though they usually focus narrowly on the death and destruction the explosion itself would cause, rather than the reverberating economic and political aftershocks. In a 2003 report, the present author and two co-authors estimated that if terrorists detonated a 10-kiloton bomb (that is, one with the explosive power of 10,000 tons of TNT, somewhat smaller than the bomb that obliterated Hiroshima) at Grand Central Station in Manhattan on a typical workday, the attack could kill half a million people and cause roughly $1 trillion in direct economic damage. 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). This was a rough estimate based on a relatively crude analysis. For more detailed recent analyses (though often focusing on attacks in areas and times with much lower population density than mid-town Manhattan on a workday) see, for example, U.S. Homeland Security Council, *National Planning Scenarios: Final Version 21.3* (Washington, D.C.: U.S. Homeland Security Council, 2006), https://www.llis.dhs.gov/sites/default/files/NPS-LLIS.pdf; Charles Meade and Roger C. Molander, *Considering the Effects of a Catastrophic Terrorist Attack* (Washington, D.C.: RAND, 2006), http://www.rand.org/pubs/technical_reports/2006/RAND_TR391.pdf; Ira Helfand, Lachlan Forrow, and Jaya Tiwari, "Nuclear Terrorism," *British Medical Journal*, Vol. 324 (February 9, 2002), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1122278/, pp. 356-358.

[12] For a useful scenario of the swirl of decision-making in the immediate aftermath of such an attack, see Brian M. Jenkins, *Will Terrorists Go Nuclear?* (Amherst, N.Y.: Prometheus, 2008), pp. 323-353.

violent, with powerful states taking unilateral action, by force if necessary, in an effort to ensure their security.

Some countries may feel that nuclear terrorism is only a concern for the countries most likely to be the targets, such as the United States. In reality, however, such an event would cause devastating economic aftershocks worldwide.[13] In 2005 then-UN Secretary-General Kofi Annan warned that these global effects would push "tens of millions of people into dire poverty," creating "a second death toll throughout the developing world."[14] The international political consequences would not be less. Hence, insecure nuclear material anywhere is a threat to everyone, everywhere.

It is implausible that terrorists would have the ability to enrich their own uranium or produce and reprocess their own plutonium. Hence, if the world's stocks of HEU and separated plutonium can be effectively secured and accounted for, keeping weapons-usable materials out of terrorist hands, nuclear terrorism can be prevented: no nuclear material, no bomb. (Conscious state decisions to provide terrorists with nuclear weapons or weapons-usable nuclear material are likely only a small part of the overall risk of nuclear terrorism, as leaders bent on maintaining their power are unlikely to take action that could provoke retaliation that would remove them from power forever.[15])

What about a nuclear sabotage? Here, unfortunately, the answers are similar. Multiple terrorist groups, including al Qaeda, Chechen terrorists, Pakistani terrorist groups, and others, have considered or actively planned attacks on reactors. While it would not be easy for terrorists to cause a major radioactive release, a variety of scenarios involving destruction of both off-site and backup power, destruction of normal and emergency cooling systems, or attacks on spent fuel pools or liquid high-level waste storage tanks have the potential to lead to large-scale releases. The Fukushima Daiichi nuclear accident highlights the scale of the terror and economic disruption such a sabotage might conceivably provoke.

In the case of sabotage, too, providing effective security against the full spectrum of plausible adversary capabilities and tactics – coupled, in this case, with strengthened safety measures that make it more difficult for either an accident or adversary action to cause a meltdown and a major radioactive release – are the most effective policy tool available to reduce the risk.

The nuclear industry itself has a huge interest in preventing nuclear terrorism. A terrorist nuclear bomb or a major sabotage of a nuclear facility would doom the industry's efforts to regain public and investor confidence after the Fukushima Daiichi accident, putting tens or hundreds of billions of dollars in future revenue at risk. Such an event, coming after Fukushima, could be the straw that broke the camel's back in some countries, leading more countries to follow in Germany's footsteps and seek to phase out nuclear power. After a terrorist nuclear

---

[13] By one estimate, the damage, reduced economic activity, defense and homeland security investments, and wars fought as a result of the far smaller 9/11 attacks cost $3 trillion. See Tim Fernholz and Jim Tankersley, "The Cost of Bin Laden: $3 Trillion Over 15 Years," *National Journal,* (May 5, 2011), http://www.nationaljournal.com/magazine/the-cost-of-bin-laden-3-trillion-over-15-years-20110505.

[14] Kofi Annan, "A Global Strategy for Fighting Terrorism: Keynote Address to the Closing Plenary," *The International Summit on Democracy, Terrorism and Security* (Madrid: Club de Madrid, 2005), http://www.un.org/press/en/2005/sgsm9757.doc.htm.

[15] Keir A. Lieber and Daryl G. Press, "Why States Won't Give Nuclear Weapons to Terrorists," *International Security*, Vol. 38, No. 1 (Summer 2013), pp. 80-104.

catastrophe, it is hard to imagine nuclear energy being able to gain the public, government, and utility support needed for it to grow on the enormous scale required for nuclear energy to be a significant part of the world's effort to respond to the challenge of climate change.[16]

The Risk of Nuclear Terrorism: A Mathematical Model

There are many ways the risk of nuclear terror might be modeled. As the issue involves a strategic interaction between terrorists seeking to make a nuclear bomb and states trying to stop them, game theory would be one possibility. Markov chains would be another obvious approach.

But so little is known about the inputs for any model that complex models that require many assumptions to make the mathematics tractable are probably not justified. For the problem of nuclear terrorism, what is needed is a simple tool that is readily understandable for policymakers, and can provide the basis for discussions of what actions to take to reduce the risk. Although it cannot provide a definitive answer about how to guard against threats, a simple model of the risk can help clarify thinking regarding nuclear security.[17]

Hence, one simple approach is to examine terrorists' chances of success on each step a terrorist group would have to take to succeed in getting and using a nuclear bomb (along each of several pathways they might choose to reach that goal), and multiply the chances at each step to get an overall estimate of the risk.[18] The chances at each step could, of course, change if the defender's policies or the terrorists' capabilities and tactics changed. 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.

The model is based on the decisions, successes, and failures of particular terrorist groups making attempts to get a nuclear bomb. Each such group has to decide how much of its efforts and resources to focus on nuclear acquisition attempts as opposed to other activities. In the model, this decision is reflected in both the number of acquisition attempts the group makes and the chances that the group will succeed at various steps. Clearly a group that devotes substantial resources to recruiting and training relevant experts, carrying out experiments, and the like will have a higher probability of being able to turn stolen nuclear material into a bomb than a group that treats the effort as an after-thought.

---

[16] To provide even a tenth of the carbon emission reductions the world is likely to need by 2050, the world would have to shift from adding roughly four nuclear plants worldwide every year during the first decade of the 21st century to 25 plants every year from now until 2050, meaning that nuclear energy would somehow have to become much *more* attractive to those choosing what power plants to build than it was before the Fukushima accident – an enormous challenge. For a pre-Fukushima discussion of the scale of growth required and steps that might enable such growth, see Matthew Bunn and Martin B. Malin, "Enabling a Nuclear Revival – And Managing Its Risks," *Innovations: Technology, Governance, Globalization*, Vol. 4, No. 4 (2009), http://belfercenter.ksg.harvard.edu/publication/19682/, pp. 173-191.

[17] A somewhat different version of this model first appeared in Matthew Bunn, "A Mathematical Model of the Risk of Nuclear Terrorism," *Annals of the American Academy of Political and Social Science*, Vol. 607 (September 2006), pp. 103-120.

[18] 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*, Vol. 22, No. 3 (June 2002), pp. 421-423.

Once a group decides to attempt to get a nuclear weapon or the materials needed to make one, they have four possible pathways to choose from (each of which, of course, represents a broad class of possibilities):

- attempting to buy a nuclear weapon or weapons-usable material that others have already stolen and are making available on a nuclear black market;
- carrying out or instigating an insider theft at a nuclear facility or transport leg;
- carrying out or instigating an outsider theft; or
- attempting to convince a state to provide a nuclear weapon or weapons-usable material.

Each of these pathways, once chosen, offers some probability of success; those chances may differ for different groups, times, and places. 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 – but grouping all possible acquisition paths into these four categories is itself a simplification.[19]

If the group does succeed in getting the material for a bomb, the group then has some probability of succeeding in turning that material into a workable nuclear bomb – that is, one that would really go off when the group wanted it to. If the group managed to build a workable bomb (or figure out a workable means to detonate a stolen nuclear weapon), it would then have some probability of choosing to, and being able to, deliver the bomb to a target location and setting it off. In this simple model, each terrorist group seeking nuclear weapons, and each individual attempt to acquire nuclear weapons or weapons-usable nuclear materials, is assumed to be independent of the others.

For simplicity, some important steps a terrorist group might have to accomplish are combined into one stage in this model. For example, getting weapons-usable nuclear material via outsider or insider theft would involve not only the theft itself, but eluding pursuit if the theft were noticed and transporting the material – probably across borders – to wherever the work on making a nuclear bomb from it was going to take place. Similarly, "bomb-making" would involve recruiting people for the effort (or training people who were already members of the group), getting relevant equipment, providing sufficient funds, and sustained management of the effort over time. Many of those individual pieces of this step might have their own signatures that might be detected.

Table 1 outlines two plausible sets of numerical values for the different elements of the model. Example 1 is somewhat pessimistic, while Example 2 is somewhat optimistic. In Example 1, there are two plausible nuclear terrorist groups. Each of them has a 30 percent chance each year of making a serious attempt to acquire a nuclear weapon or weapons-usable material.[20] (In general, each terrorist group, and indeed each acquisition attempt, would have different characteristics; the two groups in the example are the same only for clarity of exposition.) When they do make such an attempt, there is a 50 percent chance that they will choose to try to get their items from a nuclear black market (and a 20 percent chance they would

[19] In many cases, for example, outsiders and insiders might work together.

[20] Modeling the process as discrete attempts that either succeed or fail is itself a simplification; a group may be continuously seeking nuclear materials, exploring contacts, trying to find sellers who really have material, trying to find insiders with the access needed to steal material who can be recruited, and the like.

succeed on that route). There is a 30 percent chance they would instead choose to try to instigate an insider theft (and again a 20 percent chance they would succeed if they chose that option). There is only a 15 percent chance they would choose to instigate an outsider theft (with only a 15 percent chance of success on that path). The least likely choice, at only 5 percent (with a 10 percent chance of success) would be attempting to get a state to provide a nuclear weapon or the materials needed to make one. Even a 0.75% chance over 10 years is far too high a risk of a city being devastated by a terrorist nuclear bomb.

With two groups each having a 30 percent chance of making an acquisition attempt each year, the 10-year probability of a nuclear terrorist attack would be 27 percent. Thus, assumptions similar to these would support estimates made by some analysts of a 20–50 percent probability of nuclear terrorism over the next decade.[21] A risk that high is surely unacceptable, and would be worth the international community doing "everything in our power," as U.S. President George W. Bush put it, to reduce the risk.

Table 1: Two Plausible Examples

	Example 1	Example 2
Number of plausible nuclear terrorist groups	2	1
Yearly probability of an acquisition attempt for a group	0.3	0.1
Probability of choosing to buy material on black market	0.5	0.5
Probability black-market purchase attempt would succeed	0.2	0.1
Probability of choosing to get material by insider theft	0.3	0.3
Probability insider theft attempt would succeed	0.2	0.1
Probability of choosing to get material by outsider theft	0.15	0.15
Probability outsider theft attempt would succeed	0.15	0.1
Probability of choosing to get a state to provide material	0.05	0.05
Probability that attempt to get a state to provide material would succeed	0.1	.05
Probability of being able to make a workable bomb	0.4	0.2

[21] Graham Allison has famously estimated the risk at over 50 percent per decade. Graham T. Allison, *Nuclear Terrorism : The Ultimate Preventable Catastrophe*, 1st ed. (New York: Times Books/Henry Holt, 2004). Former Secretary of Defense William Perry has offered a similar estimate. Nicholas D. Kristof, "An American Hiroshima," *New York Times*, August 11, 2004. In a poll of national security experts published by Senator Richard Lugar in 2005, the median estimated ten-year chance of a nuclear attack anywhere in the world was 29 percent, and 79 percent of the experts believed that such a detonation was more likely to be from a terrorist group than from a state. See Richard G. Lugar, *The Lugar Survey on Proliferation Threats and Responses* (Washington, D.C.: Office of Senator Lugar, 2005), https://fas.org/irp/threat/lugar_survey.pdf.

Probability of being able to deliver and detonate bomb	0.7	0.4
Result: 10-year probability of nuclear terrorism	0.27	0.0078

The picture painted by Example 2 is considerably less frightening. In this example, there is only one plausible nuclear terrorist group, and they devote less of their resources to nuclear endeavors (and hence launch efforts to get a nuclear bomb less frequently, with less chance of success). The chances of successful acquisition of material, successful bomb-making, and successful delivery and detonation are all lower, with the probability cut in half in most cases. In this case, the chance that any particular terrorist attempt to get a nuclear weapon or the materials needed to make one would succeed would be only one in ten; the overall probability of an acquisition attempt leading all the way to the detonation of a terrorist nuclear bomb would be less than one percent.

Since there is only one group, with only a ten percent chance of making an acquisition attempt each year, the overall probability of a nuclear terrorist attack over a ten-year timeframe would also be just under one percent. if the chances of success were really this low, the risk of nuclear terrorism might drop still further, as the terrorists might well decide to focus on other types of attacks rather than nuclear efforts that would have a large chance of being fruitless.

But while it is *possible* that the risk is in fact this low, there are few grounds for *confidence* that this is the case. The nations of the world should take urgent steps to reduce the risk, to ensure that it moves far below the level described in Example 1 – and stays low for decades to come.

Comparing Nuclear Safety and Nuclear Security Risks: The Historical Record

What can the historical record tell us about the likely frequency of theft or sabotage at nuclear facilities, and how these compare to accident risks? Consider, first, the frequency of major accidents. The U.S. Nuclear Regulatory Commission's safety goal for nuclear reactors is that they should have a probability of major core damage of no more than one in 100,000 reactor-years of operation, and a probability of a major release of no more than one in a million reactor-years of operation. Many other countries have adopted similar goals.

Obviously, nuclear reactors around the world have not met this goal. In roughly 16,000 reactor-years of operation worldwide since 1945, four reactors have suffered major releases (one at Chernobyl and three at Fukushima Daichi) – one every 4,000 reactor-years.[22] That is 250 times as frequent as the goal. There have been a number of other major core damage events, ranging from Three Mile Island to Fermi I.

Yet the goal of reducing the probability of a major radioactive release to one in a million per reactor-year remains an appropriate objective. Given the horrifying consequences, the goal for preventing a nuclear terrorist attack on a major city should be even *more* stringent, and the goal for preventing reactor sabotage should at least be similar to the safety goal.

The history of nuclear theft suggests that the risk of such an event is far higher than it should be. Over the past 25 years, there have been some 7,500 facility-years of operations at the roughly 300 global facilities with HEU or separated plutonium. Over this time, there have been

[22] This is not including other events where reactor cores were damaged like Three Mile Island or Fermi I.

approximately 20 seizures of stolen HEU or plutonium (mostly from Russia). While several of the seizures may have been from the same theft, this amounts to a risk of one theft per 400 facility years. While many of these seizures were only gram quantities of material, several were kilogram quantities, and in 1998, Russian authorities blocked an insider conspiracy attempting to steal 18.5 kilograms of HEU – potentially enough for a nuclear explosive, depending on the enrichment level (which has not been publicly revealed).[23] Even if one assumes that the rate at facilities outside Russia was as much as ten times lower – which is probably not the case – such a rate would still be far too high for thefts of the essential ingredients of nuclear weapons.

The history of nuclear sabotage is similarly troubling. During the roughly 16,000 reactor-years of operation globally, there have been multiple cases of sabotage. These have included, among others:

- A case in which an insider placed explosives directly on the steel pressure vessel of a nuclear reactor and detonated them (the reactor was not yet operational);[24]
- A recent case (described in more detail below) in which an insider destroyed a reactor's turbine;
- A case in which 15 armed terrorists overwhelmed and captured the five armed guards at a nuclear facility under construction and were in full control for some time before departing when off-site response forces arrived;[25]
- A case in which rocket-propelled grenades were fired at and hit a reactor;[26] and
- Numerous cases of terrorist groups planning attacks on reactors.[27]

---

[23] See description and references in Matthew Bunn, John P. Holdren, and Anthony Wier, *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action* (Cambridge, Mass: Project on Managing the Atom, Harvard University, 2002), http://www.nti.org/media/pdfs/securing_nuclear_weapons_and_materials_May2002.pdf?_=1316466791, p. 10.

[24] The explosive attack on the pressure vessel occurred at the Koeberg nuclear power plant in South Africa in 1982, before the plant had begun operating. It was perpetrated by a white South African fencing champion, Rodney Wilkinson, in league with the African National Congress. It was not intended to cause a radioactive release, but to send a message. See, for example, David Beresford, "How We Blew Up Koeberg (. . . and Escaped on a Bicycle)," *Mail & Guardian* (South Africa), December 15, 1995. Beresford has offered a more detailed account, based on interviews with the perpetrator, in *Truth is a Strange Fruit: A Personal Journey Through the Apartheid War* (Auckland Park, South Africa: Jacana Media, 2010), 102–107. The cases mentioned in the text are part of a stream of cases that has continued for decades. Three decades ago, an NRC study identified "32 possibly deliberate damaging acts at 24 operating reactors and reactor construction sites" from 1974 to 1980–most of them attributed to insiders. See Matthew Wald, "Nuclear Unit Gets Sabotage Warning," *The New York Times*, June 8, 1983.

[25] This occurred in 1973 at the Atucha Atomic Power Station in Argentina, which was not yet operating at the time). Konrad Kellen, "Appendix: Nuclear-Related Terrorist Activities by Political Terrorists," in Paul Leventhal and Yonah Alexander, eds., *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism* (Cambridge, Mass.: Lexington Books for the Nuclear Control Institute, 1987).

[26] This was the 1982 attack on the French Superphénix reactor, perpetrated by environmental protester Chaïm Nissim (later elected to Parliament in Switzerland). Nissim fired five grenades from a Soviet RPG-7 he had acquired from terrorists, two of which hit the empty reactor and caused minor damage. For a confession from Nissim, see Chaïm Nissim, *L'amour et le Monster—Roquettes Contre Creys-Malville*, (Geneva: Editions Favre, February 2004.)

[27] U.S. troops found diagrams of U.S. nuclear power plants in al Qaeda facilities in Afghanistan, and Khalid Sheikh Mohammed, mastermind of the 9/11 attacks, has confirmed that al Qaeda considered attacking U.S. nuclear power plants. See, for example, Yosri Fouda, "'We Left Out Nuclear Targets For Now'," *Guardian,* March 2003,

In total, this is the equivalent of one major incident per 3-4,000 reactor-years (though there have been a much larger number of smaller incidents). While none of these incidents caused major core damage, they could have – and it seems clear that terrorist attacks in recent years have become more lethal and sophisticated. A frequency hundreds of times higher than the safety goal for a major release suggests that action is needed to reduce the risk, just as it is in the case of nuclear accidents.

The insider destruction of the reactor turbine occurred in 2014 at the Doel-4 reactor in Belgium. An insider – who the authorities have not managed to identify as of late 2015 – drained out all the lubricant for the reactor turbine, and the turbine overheated and was destroyed. The cost of replacing the turbine and purchasing replacement power while the reactor was down reportedly came to over $140 million. Reportedly, Belgian investigators think that this incident was not terrorism, but was related to a labor dispute at the site. But when investigators began trying to find the culprit, they discovered that almost two years before, a contractor employee, Ilyass Bougalab, cleared for access to the reactor's vital areas, had resigned – to go fight for terrorists in Syria. Bougalab was convicted in absentia of terrorist offenses, and is believed to have been killed fighting in Syria. In other words, this reactor had a terrorist in the vital area – but he was *not* the one who sabotaged the facility, since that happened long after he had left. Belgian regulatory authorities have since imposed tougher security requirements to protect against insiders, including more security cameras, two-person or three-person rule in certain vital areas, strengthened access controls, and checks to ensure that safety-critical equipment is operational before key events such as a reactor restart.[28]

Assessing the Risks of Theft and Sabotage at Particular Nuclear Facilities and Transports

These events suggest a significant global risk of nuclear theft and sabotage. But how should Japan think about whether its plutonium and HEU programs contribute to these risks in a significant way? The risk of theft from any given facility or transport operation with nuclear weapons, plutonium, or HEU depends on the probability a theft attempt would occur, the probability such an attempt would be successful (which is determined by the balance between what the security system can protect against and the capabilities and tactics of the adversaries), and the probability that if the items in question were stolen, that would lead to terrorists being able to set off a nuclear detonation (which depends on the quantity and quality of the material available to be stolen):[29]

$$R = P_{attempt} P_{success} P_{bomb-making}$$

---

http://www.theguardian.com/world/2003/mar/04/alqaida.terrorism. For a useful discussion of Chechen plans for reactor sabotage, see Vladimir Orlov, "Chechen Terrorists: In Preparation for a Megaterrorism Act" (August 25, 2004).

[28] See, for example, Erik Raspoet, "Wie is de Saboteur van Doel 4?" February 11, 2015, http://www.erikraspoet.be/?p=679; "Hoe Kan zo Iemand in Doel Werken?" *HLN.be,* http://www.hln.be/regio/nieuws-uit-lokeren/-hoe-kan-zo-iemand-in-doel-werken-a2095802/, October 21, 2014; and Robin Sayles, "Belgian Regulator Sets New Security Steps After Suspected Sabotage," *Inside NRC,* December 29, 2014. I am grateful to Tom Bielefeld for pointing out the first two of these references to me.

[29] This approach is a simplification, which does not take into account the difference in consequences between a single terrorist nuclear bomb and several.

Where:

R is the risk of nuclear theft from that location leading to terrorists getting a nuclear bomb;

$P_{attempt}$ is the probability of a theft attempt taking place at that site or transport route;

$P_{success}$ is the probability that the attempt will be successful; and

$P_{bomb\text{-}making}$ is the probability that adversaries would succeed in making a usable nuclear bomb from the stolen items (or be able to detonate a stolen nuclear weapon).

The probability of a theft attempt ($P_{attempt}$) is presumably determined by the other two variables. In other words, to the extent that they can, thieves will presumably attempt to steal wherever they judge their overall chances of success in achieving their goals to be highest. $P_{attempt}$ may also be higher at sites with widespread insider corruption and theft, or in organizations with substantial numbers of personnel sympathetic to the adversaries seeking the nuclear weapons or materials (as might be the case, for example, in Pakistan).

Hence, in assessing which facilities pose the largest risks of nuclear theft, the most critical factors are:

1. ***Security level:*** The types of adversary capabilities and tactics the security in place is able to defeat;
2. ***Adversary capability level:*** The types of capabilities and tactics adversaries (whether outsiders, insiders, or both together) may be able to bring to bear in their efforts to defeat the security systems and steal nuclear weapons or weapons-usable materials where the facility or transport leg in question is located (which range over a probabilistic spectrum of possibilities);
3. ***Material quantity:*** The amount of weapons-usable nuclear material available to be stolen (and in particular whether there is enough for a crude terrorist bomb); and
4. ***Material quality:*** 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, or to detonating the weapon posed by the type of built-in protections with which the weapon is equipped).

The insider threat is a particularly central part of any such an assessment. All of the few nuclear thefts where the circumstances of the theft are known were perpetrated by insiders or with the assistance of insiders – and it seems very likely that the other cases, involving bulk material that was never noticed to be missing before it was seized – were also perpetrated by insiders. Organizations often fail to recognize and act on seemingly obvious red flags until it is too late, or make other blunders in coping with the insider threat.[30]

Hence, any assessment of the risk of nuclear theft from a particular location must assess questions such as: how many people have access to the material? Is the material in bulk form, where some of it might be removed without detection? Is it being processed with workers having direct access to it? How strong is the insider threat protection program? What indicators

[30] Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge, Mass.: American Academy of Arts and Sciences, 2014), https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf.

are there of corruption, petty theft, economic desperation, or ideological extremism among the insiders with access to the material?

A very similar approach can be used to assess risks of sabotage, rather than nuclear theft. This would start by replacing $P_{bomb\text{-}making}$ with $C_{sabotage}$, the expected consequences of sabotage. The consequences of sabotage are themselves a broad distribution of possibilities depending on:

- The degree of success of the sabotage – ranging from minor damage to the facility to catastrophic radiation releases. As noted earlier, this would be determined in part by safety measures that make it more or less difficult to cause a major radioactive release. (Rough estimates of the likelihood of different results of a sabotage attempt would have to be made for use in an assessment of overall risk.)
- The quantity and toxicity of the radioactivity present and potentially dispersible. This will be very different, for example, for a small research reactor compared to a large power reactor.
- The potential for dispersing the material. A light-water reactor core, for example, contains a great deal of energy, which, if not properly cooled and controlled, could contribute to powering radioactive releases, as at Fukushima Daiichi. A dry spent fuel storage cask, by contrast, contains spent fuel that is already cooled enough that it does not need to be immersed in water. The main energy to disperse such material would have to be supplied by the explosives. In most cases, even an attack that succeeded in making a hole in a dry cask would cause only a small and local cleanup problem.
- The concentration and distribution of local populations. Clearly, the same radioactive release would have very different consequences if it were in a remote rural location or a dense urbarn area.

For sabotage, the factors just described largely replace material quantity and quality as factors in ar risk assessment. But as with material theft, the balance between the effectiveness of the security and the capabilities of potential adversaries would be a critical factor – with the potential role of insiders, and the protections against them, an essential element of that assessment.

Assessing the Risks of Theft and Sabotage in Japan

What would such a security assessment reveal about Japan? First, Japan has potential targets for either theft or sabotage.

Japan has nuclear material that would be highly attractive to terrorists, including both plutonium and HEU. At the 2014 nuclear security summit, however, Japan committed to eliminate some of its most attractive material, stocks of weapon-grade plutonium and HEU associated with the Fast Critical Assembly (FCA) at Tokai, and send them to the United States. As of late 2015, this operation was expected to be completed in 2016.[31] This is an important step forward, though Japan will still have some 10 tons of plutonium separated from spent fuel on its soil (and 37 tons more in Europe), along with smaller stocks of HEU. Any of Japan's power

[31] Matthew Bunn, "Eliminating Potential Bomb Material from Japan's Fast Critical Assembly," *Nuclear Security Matters,* March 24, 2014, http://nuclearsecuritymatters.belfercenter.org/blog/eliminating-potential-bomb-material-japan%E2%80%99s-fast-critical-assembly.

reactors, reprocessing plants, liquid HLW stores, or spent fuel pools could be potential targets for nuclear sabotage.

Japan faces fairly modest outsider and insider threats. Japan is a relatively homogenous society, with few likely sympathizers for mass-casualty terrorist groups. But it is important to remember several factors.

First, in the past, Aum Shinrikyo and other terrorist groups (such as the Red Army Faction) originated in Japan. Aum had a significant effort to get nuclear weapons that went entirely unnoticed until after their nerve gas attacks in the Tokyo subways.[32] While similar events in the future are probably unlikely, they cannot be ruled out.

Second, terrorists and criminals have demonstrated some degree of global reach. When al Qaeda attacked the U.S. embassies in Kenya and Tanzania in 1998, it was not because they had anything in particular against Kenya or Tanzania: it was because they identified those targets as vulnerable, and were able to send people from their base of operations to attack them. Similarly, terrorists are likely to attempt to steal nuclear material wherever they think their chances of success are best.

The non-nuclear theft from the Vastbërga cash depository in Sweden in 2009 illustrates the mobility of the threat – and the kinds of adversary capabilities and tactics that security planners have to take into account in defending nuclear material and facilities. While Sweden, like Japan, considers itself a generally safe country, a gang largely from Serbia came to Sweden and stole millions of dollars from a well-secured cash facility. carried off a theft of tens of millions of dollars. They used paramilitary tactics, arriving by helicopter and using automatic weapons and shaped-charge explosives and purpose-built equipment. They delayed police response by placing objects that looked like bombs at the police heliport and spreading "caltrops" – four-pointed spikes to puncture tires – on the nearby streets.[33] A similar operation might well succeed in stealing plutonium or HEU from a number of facilities around the world.

For these reasons, all countries, no matter how safe they believe themselves to be, should ensure that plutonium, HEU, and major nuclear facilities are at least protected against a common baseline threat that would include a modest group of well-armed and well-trained outsiders, able to operate as more than one team; a well-placed insider; and both the outsiders and an insider working together. A broad range of possible adversary tactics should be considered, from brute force (as in the Vastberga heist) to stealth to deception. Countries facing more severe threats should provide protection going beyond the common baseline.[34]

Japan has significantly upgraded its nuclear security in recent years. Before the 9/11 attacks, Japan did not have either on-site armed guards at nuclear facilities or a regulatory requirement to defend against a specified design basis threat, or DBT. Security has improved substantially since then, with both of those particular measures now in place, and the new regulatory agency established after the 2011 Fukushima Daiichi nuclear accident is in the

---

[32] See, for example,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: RAND, 2005), http://www.rand.org/pubs/documented_briefings/2005/RAND_DB458.sum.pdf.

[33] See Bunn et al., *Advancing Nuclear Security*, p. 8.

[34] Matthew Bunn and Evgeniy P. Maslin, "All Stocks of Weapons-Usable Nuclear Materials Worldwide Must be Protected Against Global Terrorist Threats," *Journal of Nuclear Materials Management*, Vol. 39, No. 2 (Winter 2011), pp. 21-27.

process of establishing stricter nuclear security requirements. Japan has established a nuclear security center of excellence, the Integrated Support Center for Nuclear Nonproliferation and Nuclear Security.[35] The United States and Japan have established a joint working group on nuclear security, which has been meeting regularly.[36] Japan has been converting research reactors to LEU and, as noted earlier, is in the process of sending the HEU and plutonium from the FCA to the United States. The Japanese expert who participated in a Harvard nuclear security survey reported that Japanese security requirements had become much more stringent in recent years, with a dramatic change in the kinds of adversaries operators have to protect against, and substantial changes in guard forces, requirements for security technologies, and testing and assessment.[37]

Nevertheless, nuclear security measures in Japan remain significantly weaker than those in some other countries – though the specific security measures now in place, for obvious reasons, are not made public.[38] Background checks to help screen out potential insiders are not yet routinely carried out; on-site abilities to respond to a well-armed, well-trained paramilitary team are modest; realistic force-on-force exercises are not yet a common occurrence. Not all of the recommendations of the Japan Atomic Energy Commission's nuclear security advisory panel have yet been implemented.[39]

Steps Japan Could Take to Reduce the Risks of Nuclear Theft and Sabotage

To reduce the risk of weapons-usable materials being stolen and falling into the hands of terrorists, states should:

- Reduce the number of facilities and transports handling such materials (resulting in fewer facility-years each year, and making it possible to achieve higher security at lower cost by protecting fewer targets); and
- Increase security for the facilities and transport that remain, against both outsiders and insiders (reducing the probability of theft per facility-year). This includes not only improving security equipment, but also strengthening security culture – the degree to which all relevant staff pay attention to security and are constantly seeking to improve it. As former

---

[35] See the Center's web page, at http://www.jaea.go.jp/04/iscn/iscn_old/index_en.html.

[36] Office of the Press Secretary, "United States-Japan Joint Working Group on Nuclear Security" (Washington, D.C.: The White House, March 24, 2014), https://www.whitehouse.gov/the-press-office/2014/03/24/fact-sheet-united-states-japan-nuclear-security-working-group.

[37] Matthew Bunn and Eben Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey* (Cambridge, Mass.: Project on Managing the Atom, Harvard University, 2014), http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf, pp. 27-30.

[38] For official discussions of physical protection issues in Japan, see Advisory Committee on Nuclear Security, *Strengthening of Japan's Nuclear Security Measures* (Tokyo: Japan Atomic Energy Commission, 2012), http://www.aec.go.jp/jicst/NC/senmon/bougo/kettei120309.pdf; Nobumasa Sugimoto, "Developing of Design Basis Threat and Current Physical Protection Measures," *Proceedings of the International Regulators Conference on Nuclear Security, Rockville, Md., December 4-6* (Rockville, Md.: U.S. Nuclear Regulatory Commission, 2012), http://www.nrcsecurityconference.org/slides/Dec4/Japan.pdf; Office of the Press Secretary, "U.S.-Japan Joint Working Group."

[39] For discussions of those recommendations, see, for exampleAdvisory Committee on Nuclear Security, *Strengthening of Japan's Nuclear Security Measures*; Kaoru Naito, "Nuclear Security Regime in Japan: Policies and Activities of Japanese Government," *Proceedings of International Nuclear Security: Enhancing Global Efforts, Vienna, July 1-5, 2013* (Vienna: International Atomic Energy Agency, 2013).

nuclear czar, Eugen Habiger once said, "Good security is 20% equipment and 80% culture."[40]

To reduce the risk of nuclear sabotage, similarly, states should provide increased protection against both outsiders and insiders, while increasing safety measures (including passive safety), making large-scale releases more difficult for saboteurs to achieve. For example, cooled spent fuel could be moved from pools to hardened dry cask storage, reducing the risk of major releases if an accident or terrorist attack drained the water from a densely packed pool and the spent fuel overheated.

Japan has already made progress in reducing the number of sites with weapons-usable nuclear material, converting some reactors to HEU. The shipment of the FCA material will be an important milestone. But there is certainly more to be done. With over 10 tons of separated plutonium already on Japanese soil and tens of tons more in Europe, Japan should seriously consider a moratorium on further reprocessing. Although the Rokkasho Reprocessing Plant (RRP) has already been built, the projected costs to operate it are enormous, and the lowest-cost option for Japan would be to close RRP and a adopt a fuel cycle based on storage followed by direct disposal of spent nuclear fuel.[41] Closing RRP would mean many tons of plutonium that would not be separated each year, greatly reducing bulk processing of weapons-usable nuclear material, and reducing the burdens on Japan's nuclear security systems. Rokkasho, if it operated, would also be a particularly dangerous target for potential sabotage, given the huge quantity of radioactivity in reprocessing wastes and in the spent fuel pool. If closing Rokkasho were a step too far, Japan could consider a policy of reprocessing only when additional plutonium is needed for fuel – that is, after existing stocks are consumed. At a minimum, Japan should implement its policy of not accumulating excess stocks of plutonium scrupulously, each year separating no more plutonium than was used the previous year, so that stocks remain stable or decline. Each of these steps would reduce the scale of plutonium separation in Japan in the near term and make the nuclear security job easier.

At the same time, Japan could further reduce theft and sabotage risks in its fuel cycle by finishing the elimination of the HEU on its soil; making plans not to fuel new reactors with HEU or plutonium; and moving cooled spent fuel into hardened dry casks (as close packing of fuel in spent fuel pools can increase the risk of radioactive releases from overheated fuel if the pool drains).

In addition to such steps to address the number of sites and the quantity of stocks, Japan should take steps to strengthen security for both nuclear facilities and weapons-usable nuclear material. Relevant steps include:[42]

- ***A stronger DBT.*** Japan should strengthen its DBT to ensure that it covers the full range of plausible adversary capabilities and tactics. Adversaries may be determined, capable, and creative, and their capabilities and tactics evolve. A design basis threat (DBT) from ten years

[40] Habiger, interview, October 2003.
[41] See, for example, Masafumi Takubo and Frank von Hippel, *Ending Reprocessing in Japan: An Alternative Approach to Managing Japan's Spent Nuclear Fuel and Separated Plutonium* (Princeton, N.J.: International Panel on Fissile Materials, 2015), http://fissilematerials.org/library/rr12.pdf.
[42] See, for example, Matthew Bunn, "Comment on Proposed Rule on Enhanced Security at Nuclear Fuel Cycle Facilities; Special Nuclear Material Transportation," Docket NRC-2014-0118, October 27, 2014, available at http://pbadupws.nrc.gov/docs/ML1429/ML14293A636.pdf, and references cited therein.

ago may not match today's threat. Adversaries may think of attack strategies the defenders have not considered that involve deception (fake uniforms, IDs, paperwork, etc.), blocking response forces (e.g., mining the road), or tunneling under or flying over defenses (routine in crimes worldwide).

- ***An investment in security culture.*** Given the importance of an organizational culture focused on security to achieving effective nuclear security, Japan should take steps to ensure that each operator handling weapons-usable nuclear materials or operating a major nuclear facility where sabotage could pose a serious danger establishes a comprehensive program to assess and strengthen security culture in their organization.
- ***Background checks.*** Japan should institute rigorous background checks (and ongoing monitoring and reviews) for all staff with access to weapons-usable nuclear material or vital areas of nuclear facilities, or involved in their security.
- ***Better insider protection.*** Japan should expand other measures to protect against insider threats (drawing in part, perhaps, on the new measures being implemented in Belgium after the insider sabotage there).[43] Japan should recognize, in particular, that processing plutonium or HEU in bulk – as occurs at a reprocessing or plutonium or HEU fuel fabrication facility – creates special risks of insider theft, as bulk material can more easily be removed without the accounting and control system noticing the theft. These materials should only be processed in bulk if world-class security and accounting procedures are in place, capable of detecting and localizing any loss of material (including a protracted theft of small amounts of material at a time).
- ***Capabilities to defeat the adversary.*** Japan should provide on-site tactical response forces at major nuclear facilities (and for nuclear transports) trained and equipped to defeat the DBT. Tests in the United States have shown that in many scenarios, off-site response forces arrive too late to prevent a sabotage or a theft.
- ***Regular, realistic testing.*** Japan should conduct regular, realistic tests of its nuclear security systems' ability to defeat intelligent, determined adversaries looking for new ways to overcome the security system – including both outsiders and insiders. This should include conducting regular force-on-force exercises for all major nuclear facilities and transport organizations.[44]
- ***Material in less attractive forms.*** To the extent practicable, Japan should store and transport plutonium and HEU mixed with other materials, so that they could not be used for a nuclear bomb without chemical processing. This would mean it would require more time and additional steps for terrorists to make a bomb if material was ever stolen, potentially offering more opportunity to recover it. But Japan should not put too much reliance on this measure,

---

[43] Bunn and Sagan, *A Worst Practices Guide*; World Institute for Nuclear Security, *Managing Internal Threats: A WINS International Best Practice Guide for Your Organization*, Rev. 1.0 (Vienna: WINS, 2010); International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, Vol. IAEA Nuclear Security Series No. 8 (Vienna: IAEA, 2008).

[44] For an attempt to outline the key elements of an "appropriate effective" nuclear security and accounting system, as required by UN Security Council Resolution 1540, see Matthew Bunn, "'Appropriate Effective' Nuclear Security and Acounting - What is it? ," paper presented at Global Initiative/UNSCR 1540 Workshop on 'Appropriate Effective Material Accounting and Physical Protection', Nashville, Tennessee July 18 2008 http://belfercenter.ksg.harvard.edu/files/bunn-1540-appropriate-effective50.pdf.

as any group capable of doing the difficult job of making a crude nuclear bomb from pure plutonium is likely to be able to do the simpler job of getting pure plutonium from, for example, a mix of uranium and plutonium.

- ***Regular, creative vulnerability assessments.*** Japan should expand its program to assess vulnerabilities at nuclear facilities. Vulnerability assessment is a difficult art. Often, if only a few of the most obvious possible adversary pathways are considered, a system may appear to be highly effective – but others with a more creative approach may find dangerous vulnerabilities. Japan should assign creative teams with a hacker mentality to probe for weak points in its security systems, and offer incentives to encourage people to identify vulnerabilities and propose fixes.
- ***Integrated cyber defense.*** In this digital age, Japan should take steps to protect its facilities not only from physical assaults or theft attempts, but from cyber attacks as well. Physical security and cyber security must be integrated, as nearly all security and accounting systems are now digital: it is essential to ensure that adversaries cannot use a cyber attack to facilitate a physical attack, by turning off alarm and detection systems, opening gates or vault doors, or falsifying accounting records to cover up a nuclear theft.

The Path Ahead

The dangers of nuclear terrorism are very real. They are likely to be with us as long as terrorists bent on mass destruction and nuclear materials and facilities both exist in the world. Simple models and historical evidence suggest that the risks of nuclear theft and sabotage may be as large or larger than the risks of nuclear accidents. To be expandable on the scale needed to make a major contribution to mitigating climate change, nuclear energy must be seen as both safe and secure.

Fortunately, straightforward steps are available that can greatly reduce these risks at reasonable cost. These include minimizing the use of materials that could be used in nuclear weapons, and providing highly effective security and accounting wherever these materials exist.