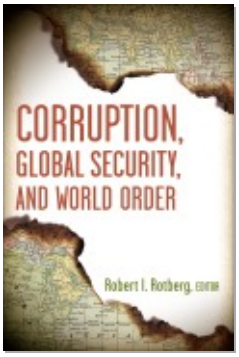
Corruption, Global Security, and World Order

Robert I. Rotberg



Published by Brookings Institution Press

MATTHEW BUNN

6 *Corruption and Nuclear Proliferation*

Corruption is a critical, under-recognized contributor to nuclear proliferation. With the possible exception of North Korea, corruption was a central enabling factor in all of the nuclear weapons programs of both states and terrorist groups in the past two decades. Indeed, corruption is likely to be essential to most cases of nuclear proliferation. Unless a state or group can get all the materials and technology needed for its nuclear weapons program from some combination of its own indigenous resources; outside sources motivated only by a desire to help that nuclear program; or outside sources genuinely fooled into providing technology that they believe is for another purpose, illicit contributions from foreign sources motivated by cash will be central to a nuclear program's success. New steps to combat corruption in the nuclear sector, and in security, law enforcement, and border control agencies that are responsible for preventing nuclear theft, technology leakage, and smuggling are essential to strengthen the global nonproliferation regime.

Of course, since corruption and proliferation are both secret activities, no precise measure of the frequency of proliferation-related corruption is available. No one knows if the documented cases represent nearly all of the cases that have occurred, or only the tip of the iceberg. This chapter uses a brief summary of the global black-market network led by Pakistan's Abdul Qadeer (A. Q.) Khan to illustrate the broader phenomenon; it lays out a taxonomy of different ways in which corruption can contribute to proliferation (or slow it, in some cases); and it offers the outline of an approach to reduce the dangers that are posed by corruption-proliferation linkages.

Defining Corruption

Transparency International defines corruption succinctly as "the misuse of entrusted power for private gain."[1] This misuse of power applies not only to corrupt public officials, but also to private employees with entrusted power: a company official who gives a lucrative contract to one supplier rather than another in return for kickbacks is clearly corrupt. Access to sensitive nuclear weapons–related technology and information also represents entrusted power. Selling that entrusted information or technology for private gain, knowing that it probably will be used to contribute to a nuclear weapons program in a foreign state, is a corrupt act—as the term is used in this chapter—even if the sellers manage to carry out their activities in locations where the laws are so weak that the sellers are not violating local law. Many of the corrupt participants in recent proliferation cases fall into this category; they did not hold public office, but rather used their access to key information, equipment, or materials (which had been entrusted to them by states, or firms acting on behalf of states) to earn millions of dollars from illicit transfers.

By this definition, for example, Peter Griffin, a British citizen, who was a key supplier of uranium enrichment centrifuge technology to Pakistan knowing full well that Pakistan would use this technology to produce nuclear weapons, would be considered corrupt, even though he did not hold public office, and even though he has long argued (perhaps correctly) that at the time of his activities, the export control laws that were in place were so weak that his activities were not illegal.[2] On the other hand, the firms that sold centrifuge-related equipment to Iraq in the apparently genuine belief that it was going to be used in the oil industry would not be considered corrupt, though they certainly had inadequate procedures in place to manage sensitive technologies. Between these extremes, there is the gray area where individuals may be able to convince themselves that nothing is amiss with a high-technology purchase, even when there are glaring signs of proliferation intent—which is the reason why many countries' export control laws limit exports that the exporter "knows *or has reason to know*" will be used for illicit weapons programs.[3]

By this definition, people who spied—that is, provided entrusted information—for cash would be considered corrupt, but people who spied or transferred sensitive technology and materials because they believed in the cause of those who they were helping would not. In the case of major transfers of information, equipment, and materials for nuclear weapons, however, this definition does not provide a limitation. While there have been ideological rationalizations involved in technology transfers, all of the major transfers

considered in this chapter appear also to have involved substantial amounts of money that has gone into the pockets of corrupt participants. Transfers that are made on these scales are rarely done for free.

An Illustrative Case: The A. Q. Khan Network

As is now widely known, Pakistan's Khan led a global black-market nuclear technology network that operated for two decades. It marketed uranium enrichment centrifuge technology to Libya, Iran, North Korea, and possibly to others. The network also provided items such as a detailed nuclear bomb design (to Libya, and possibly to others) and instructions on casting uranium metal into the hemispheres that are useful for bomb components (to Iran, and possibly to others).[4] Corruption was fundamental to everything that the network did.

The operation began when Khan, who had been employed at a firm that was a subcontractor for the European enrichment consortium Urenco, left the Netherlands for Pakistan with centrifuge designs, photographs, a list of key suppliers, and a web of personal contacts. His initial theft of the centrifuge designs appears to have been motivated primarily by nationalism, and hence should not, by the definition above, be considered an act of corruption. However, the act was certainly illegal, and Khan's personal ambition played a role. Once back in Pakistan, Khan eventually convinced Prime Minister Zulfiqar Ali Bhutto that Pakistan would need to corrupt a wide range of suppliers to get covert, illegal supplies for its centrifuge program and, therefore, that Khan would have to control personally "large sums of money" with the freedom to "spend it without anyone looking over [his] shoulder."[5]

This arrangement, which continued in various forms for decades, succeeded in its intended purpose. Using this cash and Khan's network of contacts among European centrifuge technology suppliers, Khan and his Pakistani colleagues succeeded in corrupting many suppliers and buying key components and materials such as maraging steel (a difficult-to-make specialty steel with the high strength that is needed for fast-rotating enrichment centrifuges). Friedrich Tinner, Henk Slebos, Gotthard Lerch, Gerhard Wisser, Daniel Geiges, and Peter Griffin were among the most important of those who provided sensitive information and technology in return for cash—each individual's acts clearly meeting any reasonable definition of corruption. (Many of these individuals, however, have never been jailed, were jailed only briefly, or were not jailed until years after the network had been disrupted, either because of a lack of evidence that could be produced in open court or

because the export control laws in the countries where they were operating were so weak that their exports were not illegal at the time.)

The large flows of cash to Khan, with little accountability, also led to corruption in Pakistan. As the years went by, Khan, despite having a modest government salary, became well-known for his wealth and power.[6] Moreover, Khan reportedly used large sums of cash to pay off a range of military personnel and government officials (including a succession of officers that were charged with security at the A.Q. Khan Research Laboratories, Pakistan's main facility for enriching uranium for its nuclear bomb program), to subsidize dozens of reporters for favorable coverage, and even to create prizes that were then awarded to Khan. Decades later, when President Pervez Musharraf established the National Accountability Bureau to help address corruption in the Pakistani government, the bureau developed a remarkable 700- to 800-page dossier on Khan's corruption. The documents reportedly confirmed that Khan owned at least nine houses in Pakistan and London that were worth millions of dollars; controlled bank accounts that contained some $8 million in several countries; and also owned a hotel in Timbuktu, named after his wife, to which a Pakistani Air Force cargo plane had delivered a load of furniture. In addition, the papers detailed a range of corrupt transactions, in which Khan had personally skimmed 10 percent from procurement contracts for the A.Q. Khan Research Laboratories or had arranged to purchase far more of certain expensive items than the laboratory needed, apparently selling the rest for profit. (The laboratory—which includes the enrichment plant that produced the highly enriched uranium [HEU] for Pakistan's bomb—was renamed in Khan's honor.) Despite such overwhelming evidence, the bureau decided not to bring a case against Khan because he was so powerful, and the corrupt network that he had established penetrated so far within the Pakistani establishment that attempting to prosecute him might have brought down the National Accountability Bureau.[7]

Having successfully corrupted European and other suppliers to get what they needed for Pakistan's program, Khan and his co-conspirators then turned their network into an export enterprise, supplying centrifuge technology and other nuclear weapons–related technologies to Iran, Libya, and North Korea (to name the documented cases).[8] There are continuing controversies over the extent to which any or all of these transfers were authorized by the Pakistani government or high-level officials other than Khan; officially, the Pakistani government asserts that no senior officials except Khan were involved. Since the operation included steps such as removing entire centrifuges from the Khan Research Laboratories and flying them to

foreign countries on Pakistani military aircraft, accepting the assertion that the operations were unauthorized leads to the conclusion that security failed on an epic scale, representing a remarkable level of success for Khan in corrupting others to take part in this scheme.[9] In all likelihood, there was a combination of authorization and corruption that penetrated deeply into the Pakistani military and security establishment. There are strong suggestions, for example, that the initial transfers to Iran were authorized by General Aslam Beg, then the chief of army staff, less so for cash than to build a strategic anti-Western alliance.[10] Ultimately, the high-level positions of those who probably participated in the network raise the question of "state capture"—corruption so deep that on some key issues, the corrupt participants can control the policy of the state.[11]

Whatever the case, it is clear that corruption was an essential element of this entire operation. Many of the same corrupted suppliers who had provided technology and equipment to Pakistan then did the same for the network's other clients, and they and Khan reportedly earned millions of dollars in the process. Gotthard Lerch, for example, reportedly initiated the network's first dealings with Iran in the 1980s, arranging for the network to provide centrifuge designs and components in return for $10 million, of which Lerch pocketed $3 million.[12] Ultimately, individuals or firms in some twenty countries participated in what was truly a global network. Most of these participants were corrupted, knowingly providing technologies that would contribute to nuclear proliferation for cash. Admittedly, some may have been genuinely unaware of the real end use of what they were providing. For example, managers of the Scomi plant in Malaysia, which was making key centrifuge components for Libya's program, claim that they believed that the parts that they were making were for the oil industry.[13]

In the end, foreign intelligence services managed to penetrate the network (turning at least one of the corrupted participants, Urs Tinner, son of one of Khan's original suppliers). Foreign governments seized a ship that was filled with centrifuge parts that was headed for Libya. The Libyan government, in the process of giving up its nuclear and chemical weapons programs, provided detailed information on its dealings with the network. Musharraf forced Khan to make a televised confession and placed him under house arrest. Khan, however, remains a revered national hero in Pakistan and was released from house arrest with no charges against him in early 2009. Only a few of the other Pakistani participants were ever detained, and, as far as is publicly known, none are still in custody. Only a few of the participants that are located elsewhere have spent time in jail; most remain free.

A Taxonomy: Corruption-Proliferation Linkages

The proliferation programs of states and of terrorist groups are generally different, given the far greater technical and financial resources that a state can bring to bear, and states' and terrorists' different goals. Typically, a proliferating state wants an arsenal of safe, reliable weapons that can be delivered by missile or aircraft and that can be stored for a long time, to act as a deterrent. A terrorist group, by contrast, may be satisfied with one or two crude, unsafe, unreliable weapons that fit in a minivan.

In particular, proliferating states typically seek the technology to make their own nuclear bomb material (though they may also seek ready-made bomb material as a complementary short-cut). In recent years, easy-to-hide uranium enrichment centrifuges have been the technology of choice for the determined nuclear cheater.[14] Because the export of this technology from states that had it to potential proliferatant states was generally banned, corrupting people to convince them to sell illicitly is fundamental to these programs. States have also sought nuclear weapon designs, nuclear weapon manufacturing technology, and more. A typical procurement transaction might involve several stages, each of which might require cash to grease the skids. These stages can include:

—Convincing an individual or firm to provide sensitive technology, equipment, or materials;

—Bypassing or gaining approval from whatever internal review process may exist at the firm;

—Bypassing or gaining approval from whatever export control system the country may have; and

—Bypassing or gaining approval from customs and border control officials.

For terrorists, by contrast, making their own nuclear bomb material is simply out of reach.[15] Unfortunately, however, if terrorists succeeded in getting plutonium or HEU, making a crude nuclear bomb, while a substantial challenge, is not as difficult as many believe, and is within the plausible capability of a sophisticated terrorist group.[16] Aum Shinrikyo and al Qaeda, the two terrorist groups whose efforts to get nuclear weapons have been the most substantial and well documented to date, both sought to get either stolen nuclear weapons or stolen nuclear materials that could be used to make a bomb and to recruit or otherwise acquire the expertise that was needed to make a bomb.[17] In both cases, a key approach was to offer large sums of cash to people who might have had access to such items to get them to agree to

provide them. Aum Shinrikyo, for example, reportedly attempted to arrange a meeting in Russia with then-Minister of Atomic Energy Victor Mikhailov, to offer him $1 million for a nuclear warhead—a clumsy approach that certainly would not have worked.[18] Aum Shinrikyo's "Construction Minister," Kiyohide Hayakawa, traveled repeatedly to Russia, buying a wide range of weapons and technologies (including a military helicopter, which was shipped to Japan for the cult's use). One of Hayakawa's notebooks from these trips includes the notation "how much is a nuclear warhead?" followed by several possible prices.[19]

As in the case of a state, a procurement effort by a subnational group that is seeking a nuclear weapon or the materials to make one would typically proceed in several stages, all of which might be facilitated by corruption. The stages involve:

—Convincing an individual or group to steal the desired items (or to help others to do so, for example, by turning off alarms or providing detailed information on security arrangements); or

—Convincing an individual or group to sell already-stolen items; and

—Bypassing or gaining approval from customs and border control officials.

An examination of the relevant cases suggests that the two most important types of proliferation-related corruption include technology experts who corruptly provide sensitive technology (especially centrifuge technology) to states, and nuclear staff or security and border officials who participate in or facilitate theft and smuggling of nuclear materials, possibly for terrorist groups. Below is a brief taxonomy of the different stages of proliferation efforts that are carried out by states or subnational groups in which corruption may play an important role.

Corrupt Provision of Sensitive Information, Technology, or Equipment

Corrupt provision of sensitive information, technology, or equipment appears to be the most common form of proliferation-related corruption, and it has been a factor in every state nuclear weapons program in recent decades. Iraq's extensive successes in corrupting suppliers in Europe, the United States, and elsewhere have been well documented; in many respects they parallel Pakistani successes. Individuals and firms in Europe, the United States, and elsewhere provided a wide range of centrifuge designs, components, flow-forming machines for manufacturing centrifuges, etc. Some of these firms and individuals apparently were unaware of the purposes for which their technologies would be used, but others actively helped to forge end-user certificates, falsify

export forms, and the like. Two corrupt individuals played particularly crucial roles in Iraq's program: German engineer Bruno Stemmler provided detailed centrifuge design drawings, stolen centrifuge components, and extensive personal assistance to Iraq in return for just over $1 million; Karl-Heinz Schaab provided more advanced centrifuge designs, techniques for manufacturing key components, machines for testing and balancing centrifuges, and on-site technical help that accelerated the Iraqi program "by many months, if not years," in return for millions of dollars.[20] Iran, Libya, and North Korea all convinced suppliers to provide them with controlled technologies in return for large sums of cash. The suppliers, in most cases, knew full well that the technologies would be used for nuclear weapons.

Further, people who have critical proliferation-sensitive knowledge that have left the agencies, firms, or institutes where they acquired that knowledge pose a particularly difficult control problem that is not addressed by many current non-proliferation programs.

Many of the most important corrupt technology suppliers fall into this category. When Stemmler was introduced to the Iraqis, he was "embroiled in a conflict" with his employer and looking to leave, having already been forced out as head of the company's isotope separation lab "in a manner that left him embittered and angry."[21] He left the firm, apparently stealing extensive documentation and nuclear components in the process, and sold his knowledge to the Iraqis. Schaab, recruited for the Iraqi effort by Stemmler, had left the same centrifuge firm of his own accord, also "bitter" about how he had been treated there.[22] While Gotthard Lerch was working for Leybold-Heraeus in Germany when he began supplying Khan, he was forced to resign after the government questioned his dealings with Pakistan; he moved to Switzerland in 1983 and continued to supply the Khan network for two decades from there.[23] This history suggests that it is time to reconsider current policies that ignore personnel who have left their institutes or firms in programs intended to redirect weapons scientists to civilian work and that impose few constraints on individuals who previously had authorized access to highly sensitive technologies.

In some cases, the corrupt suppliers in these transactions were individuals; in others entire firms or institutes were involved. A prominent example is H+H Metalform GmbH, in which Iraq secretly bought a major share, and that provided a wide range of centrifuge-related technologies and materials.[24] Similarly, Iraq secretly acquired the British precision machine tool firm Matrix Churchill, which became a central element of Iraq's illicit procurement program.[25] In another troubling case, even after the 1991 imposition of United Nations sanctions that banned all transfers of long-range missiles or

components, Iraq succeeded in convincing Russian institutes to provide a wide range of missile technologies to Iraq, including missile guidance equipment that was taken from dismantled Russian strategic submarine-launched ballistic missiles (SLBMs) and was tested and certified as functioning properly by one of Russia's key missile institutes.[26] As this act was in direct violation of Russian export control laws and UN sanctions, to which Russia was a party, in return for cash to the institutes (and perhaps to individual managers there), this transaction was clearly corrupt. These cases may represent a situation in which a few corrupt individuals at a firm convinced the rest of the firm to move ahead with a particular transfer, thereby putting the reputation of the entire firm at risk.

Corrupt Provision or Theft of Sensitive Materials

Provision of materials is closely related to provision of information, equipment, and technology. In the case of nuclear weapons programs, the materials in question may be materials that are needed to manufacture equipment that produces nuclear bomb material (such as the high-strength maraging steel for centrifuges that was mentioned above), or they may be the nuclear bomb materials. (The key materials that can be used to fuel the nuclear chain reaction in a nuclear bomb are plutonium or HEU.[27])

Corrupt provision of materials such as maraging steel has been a factor in (at least) the Pakistani, Iraqi, and Iranian nuclear programs. The Iraqi purchase of 100 tons of maraging steel—estimated by Mahdi Obeidi, the purchaser, as enough for 10,000 centrifuges, capable of producing material for 15 nuclear bombs a year—was so clearly understood as corrupt by all participants that some of the key discussions took place in a strip club in Paris.[28]

There have been numerous cases (primarily in the 1990s) of authorized insiders stealing plutonium or HEU with the intention of selling it on the black market. By the definition above, these individuals would be considered corrupt, since they were misusing entrusted access to these materials in the hopes of private gain. The public record, however, does not yet include successful cases in which potential buyers corrupted existing insiders at facilities where plutonium and HEU existed and convinced them to steal it for them—that is, cases where the theft took place at the instigation of a known buyer. In at least one case, intelligence agents posing as buyers may have provoked a theft of nuclear material in this way: in 1994, the 363 grams of plutonium seized at the Munich airport from a flight that came from Moscow was the result of a sting operation by German intelligence (though the public record is not clear on whether the sting provoked the theft or the thieves already had the material when the sting began).

More recently, there was a clear attempt to corrupt insiders to steal bomb material. During 2003, proceedings in a Russian criminal case revealed that a Russian businessman had offered $750,000 for stolen weapons-grade plutonium for sale to a foreign client, and he had made contact with residents of the closed nuclear city of Sarov, home of one of Russia's premier nuclear weapons laboratories, to try to secure a deal.[29] Two Sarov residents received $50,000 up-front from the Nizhny Novgorod businessman, Boris Markin, with the promise of the rest to come when the plutonium was delivered. Fortunately, the two were scam artists with no access to plutonium. Oddly, though his effort to get stolen plutonium was a grave crime under Russian law, when the two men made off with his down payment, Markin went to the local branch of the Federal Security Service (FSB, from its Russian title, the successor to the KGB) and charged the two with fraud—perhaps fearing his client, whose money he had spent, more than he feared the Russian security services.[30] As the investigation was underway, Markin was hit by a car and killed. While Russian investigators concluded that his death was an accident, with no relation to the case; suspicions remain. Although no actual plutonium was stolen, this incident is particularly troubling in that it demonstrates the existence of Russian businessmen with substantial sums of cash and connections to clients abroad seeking to buy weapons-grade plutonium and knowledgeable enough to begin making contact with residents of closed nuclear cities to do so.[31]

Groups such as al Qaeda have made repeated efforts to buy already-stolen nuclear material, though there is not yet public evidence that they have actively attempted to corrupt individuals to carry out such theft. In the early 1990s, for example, al Qaeda sought to purchase what it believed to be HEU from a smuggler in the Sudan, though this transaction appears to have been a scam. As recently as 2003, U.S. intelligence received "a stream of reliable reporting" that al Qaeda operatives in Saudi Arabia were negotiating for the purchase of three Russian nuclear warheads.[32] Indeed, efforts to corrupt people who might be able to provide nuclear weapons or materials have been fundamental to all of the known terrorist efforts to acquire nuclear weapons to date.[33]

Corrupt Assistance in Sensitive Materials Thefts

Of course, corrupt insiders might not carry out a theft of potential nuclear bomb material, but instead might only assist in the theft—leaving a back door open, turning off a crucial alarm, providing information about security system weaknesses and exactly which material to take, etc. In a 1993 case at the Sevmorput Naval Shipyard, for example, Dmitry Tikhomorov, an employee at the yard, told his brother, a retired naval officer, about security weaknesses

there, assisting his brother in stealing 4.5 kilograms of uranium enriched to approximately 20 percent U–235.[34] In the United States and in a number of other countries, the "design basis threat" that nuclear security systems are required to protect against includes the possibility of an insider providing this sort of assistance to thieves.[35]

Such corrupt assistance can take many forms and can require many levels of knowledge on the part of the corrupted individuals. In Russia, for example, the largest nuclear weapons facilities are located in "closed cities," with a fence around the entire city that is guarded by armed troops. No one may enter the city without approval from Russian authorities, and everyone going in or out is checked by the guards. A U.S. study based on interviews with residents of one of these cities, however, found that the cost of bribing a guard to gain access to the city without being checked amounted to a few dollars or a bottle of vodka.[36] In mid-2006, Russian President Vladimir Putin fired the Ministry of Interior's (MVD) Major-General Sergei Shlyapuzhnikov, who was the deputy commander of the MVD department that was charged with law and order in the closed cities; according to the Russian state newspaper, he was fired for organizing smuggling in and out of those cities and handing out passes that allowed people and vehicles to enter and leave without being checked.[37] By allowing unchecked passage, such corrupt officials could create major pathways for nuclear theft and smuggling without realizing that they were contributing to anything more than low-level smuggling of cigarettes and pirated CDs.

Corrupt guards at nuclear sites pose a particular risk. In 2003, Igor Goloskokov, then the chief of security at Seversk (formerly Tomsk-7), one of Russia's largest plutonium and HEU facilities, warned that the MVD troops that were guarding the site were poorly paid, poorly trained, and frequently corrupt, becoming "the most dangerous internal adversaries."[38] This situation is of particular concern since a survey of a wide range of thefts from guarded facilities found that the guards were frequently among the thieves.[39] Corruption in the military and security services that are charged with guarding nuclear stockpiles is widespread in Russia and in Pakistan and has included corrupt assistance to terrorists.[40]

Corrupt Hiring that Provides Access to Sensitive Technology or Materials

There are many institutions in many countries where jobs are for sale. This circumstance can create major opportunities for those seeking to access a site's technology or materials to infiltrate the institution by buying their way in. When a hire means money into the hiring official's pocket, there is a strong

incentive not to do an in-depth background check. In one study, for example, U.S. researchers, working with Russians living in the closed nuclear city of Ozersk, home of the Mayak Production Association, one of Russia's largest plutonium and HEU processing facilities, were able to develop rough estimates of the cost of purchasing a wide range of jobs at the Mayak complex.[41]

Corrupt Financing of Sensitive Transfers

Many of the transfers of sensitive nuclear weapons–related technology that are described above involved the exchange of millions or tens of millions of dollars. The witting or unwitting participation of major banks in financing the transactions was essential. In many cases, the banks, where accounts and wire transfers were used, had no knowledge of the illicit transactions and cannot be considered corrupt. Other banks, however, were clearly complicit. Iraq's program established a special relationship with the Atlanta branch of the Banca Nazionale de Lavoro (BNL), a bank that is owned by the Italian government, with branches all over the world. BNL handled billions of dollars in Iraqi funds and financed a wide range of illicit purchases. Atlanta branch manager Christopher Drogoul and five other employees were subsequently charged with conspiracy, wire fraud, and related crimes.[42] Similarly, the Bank of Credit and Commerce International (BCCI)—a bank renowned for its deep corruption—played a central role in financing the activities of the Khan network.[43]

Corrupt Approval of Sensitive Transfers

In some cases, individuals or firms that provide sensitive technology, equipment, or materials simply smuggle it across borders without seeking any type of permission. In other cases, corrupt participants falsify documentation to get shipments through customs or export control processes. On occasion, the officials charged with reviewing and approving or rejecting high-technology exports may be bribed to approve illicit shipments. In the case of the transfers of Russian ballistic missile guidance to Iraq, for example, at one stage a Russian customs official reportedly raised questions about the low declared value of a set of boxes that contained missile guidance equipment, but he approved the shipment in return for a bribe.[44] It seems likely that the frequency of this type of corruption is far greater than is known.

Corrupt Approval of Border Crossings

Customs and border control officials in many countries are notoriously corrupt. The responsibility to oversee what can and cannot be brought across a border, often at remote posts, with little oversight, creates opportunities for

corruption to flourish. The possibility that contraband can get past borders in return for a modest bribe poses a fundamental problem for efforts to block illicit transfers, whether of nuclear materials, nuclear technologies, or drugs and other contraband.

In the case of preventing nuclear smuggling, donors have long recognized that there may be little value in providing radiation detection equipment to officials if those using it can easily be bribed to ignore an alarm.[45] In a significant case in 2006, stolen HEU had reportedly been smuggled from Russia to Georgia with the aid of a corrupt border official who was a relative of the principal smuggler, Oleg Khintsagov.[46]

Similarly, in late 2004, Russian authorities revealed that they had launched an investigation into a smuggling ring that was apparently run by customs inspectors at the Russia-Finland border checkpoints of Torfyanovka and Brusnichnoye. In 2003, the smugglers allegedly allowed 1,356 cargo trucks to pass through the checkpoint without paying the requisite duties, costing the state a total of $30 million in uncollected fees. Andrej Andreyev, the head of the Torfyanovka checkpoint, was fired as a result of the ongoing investigation. Although this ring does not appear to have been involved in nuclear smuggling, such an organized ring of corrupt customs officials can create important opportunities for smuggling nuclear materials or technologies.[47]

Corrupt Protection of Proliferation Activities and Networks

Organized crime groups and criminal networks regularly infiltrate police forces, or they corrupt members of the police around the world, allowing these groups to be warned of impending searches or arrests. In some cases, judges are corrupted to protect criminal networks as well. It is not clear from the public record whether proliferation networks have paid for such protection. It seems likely that Khan's extensive corrupt network in Pakistan provided important warnings and protection that allowed some of the network's illegal activities in Pakistan to continue longer than they otherwise would have.

Corrupt Interference in Non-Proliferation Programs

Over the years, the United States and other countries have spent billions of dollars on programs to fix some of the weaknesses that corrupt proliferation participants have exploited—helping states upgrade security for nuclear stockpiles, strengthen export controls, and more. Corruption has certainly slowed and interfered with these efforts—not surprising, as non-proliferation programs have been implemented in some of the world's most corrupt countries, from the former Soviet Union to Pakistan.

The most infamous case is that of Evgeniy Adamov, Russia's former minister of atomic energy. In 2008, Adamov was convicted of taking part, with others, in stealing 62 percent of the shares (a value of some $31 million) of a joint venture that was involved in implementing the U.S.-Russian HEU Purchase Agreement.[48] U.S. prosecutors have charged Adamov with stealing $9 million from U.S. funds that had been provided to upgrade nuclear safety at Russian reactors. The U.S. officials who oversee that program have pointed out that the nuclear safety work that they paid for was completed, so if Adamov stole money, it was from the people who did the work and did not get paid as much as they should have, not from the United States.[49] Corruption was reportedly a commonplace feature of Adamov's activities during his tenure at the ministry.[50]

Adamov's case is by no means an isolated one, however. Corruption is endemic in key ministries with which foreign non-proliferation programs have had to work. As one example, Russian sites must get approval from Rosatom (the institution that replaced the Ministry of Atomic Energy, which is now a state corporation) for U.S.-funded contracts to upgrade nuclear material security and accounting systems. These approvals are often delayed at headquarters for months at a time. But the headquarters' official charged with approving these contracts told an expert from one Russian site that they could be approved in a week or two if he paid an expediting fee of a few percent of the contract value to a private firm (owned by people close to the official making the suggestion).[51]

In another instance where at least suspicions of corruption slowed down non-proliferation cooperation, in the early 1990s, the United States and Russia disagreed over the design for a massive, secure storage facility for material from dismantled nuclear weapons, which was to be built at Mayak. The institute that designed the building refused to provide the design and allow the project to begin until it had been paid $1 million that it was owed for its work, and the Ministry of Atomic Energy claimed to have no money to pay it. The U.S. Department of Defense (DOD), which was funding the project, refused to pay, arguing that Russia's willingness to do so was an indicator of whether Russia was serious about paying its agreed share for the cost of the project. After months of delay, the U.S. Department of Energy (DOE) agreed to pay to avoid continued delays. The question then arose of how the money should be transferred. Victor Mikhailov, Adamov's predecessor as minister of atomic energy, provided a bank account in an off-shore banking haven in Europe and suggested that the money be sent there. Given the chaos in the Russian banking system at the time, it is quite possible that this was a legitimate ministry

bank account, but Mikhailov's suggestion did not meet "the smell test," and ultimately, the U.S. government dispatched U.S. officials to carry cash directly to the design institute.[52]

Corrupt Permissions that Allow Control Weaknesses to Continue

In many cases, weaknesses that might be exploited by those seeking nuclear materials or technology would be expensive to fix, which creates a potential incentive to use bribery to avoid having to fix them. In Russia, for example, nuclear security inspectors for Rostekhnadzor, the agency charged with regulating security and accounting for non-military nuclear material, are paid only a few hundred dollars a month. If they find a significant violation of nuclear security or accounting rules, the cost of fixing those violations in many cases is hundreds of thousands or millions of dollars. The potential incentive to bribe the inspector to overlook the problem is obvious. In 2008, a Russian MVD colonel was reportedly arrested for soliciting thousands of dollars in bribes to overlook violations of security rules in the closed nuclear city of Snezhinsk.[53] While this appears to be the only case of bribery of this type of official in the public record, bribery of virtually all other types of inspectors is commonplace in Russia.

Domestic Corruption as an Obstacle to Proliferation Success

As with any other large-scale project that a government undertakes, corruption can also interfere with nuclear, chemical, or biological weapons programs. While there is no evidence that Khan's extensive corruption slowed the Pakistani nuclear weapons program, it certainly made it more costly. In Iraq, under Saddam Hussein, corruption permeated virtually every major program. While corruption related to the oil-for-food program helped to finance illicit procurement after the 1991 war, corruption and empire-building by the technical leaders of the weapons program may also have distorted and slowed the effort. Covering some 35,000 m^2, for example, the immense nuclear weapons development and testing facility at Al Atheer appears to have been far larger than many reasonable estimates of the need.[54]

Corruption and Proliferation: What Is The Role of Organized Crime?

Corruption and large, established organized crime organizations are often conceived of as integrally linked. But in the case of nuclear proliferation, it appears that there are many cases of corruption that do not involve anything resembling traditional Mafia-style organized crime groups.

Clearly, the Khan network and the illicit procurement networks that were put together by Iraq, Iran, and others represent organized operations that relied heavily on corrupting potential suppliers and were, in some of their activities, criminal. Yet there is little evidence in the public record that traditional organized crime groups played any substantial part in these proliferation activities. These proliferation networks focused on corrupting a rarefied world of experts in advanced technologies who typically had little to do with the ordinary criminal world.

With respect to the smuggling of nuclear and radiological materials, there is an ongoing debate about the past and potential future role of organized crime. On the one hand, the known cases of smuggling of plutonium or HEU have generally not involved organized crime. Indeed, they have often involved what might be called comically disorganized crime—thieves who stole nuclear material with no particular idea about how to find a buyer, incompetent middlemen who had no idea what to charge for nuclear material or how to move it, and so on.[55] A detailed analysis of both nuclear cases and the much larger number of cases involving radiological materials suggests that only about 10 percent of the total number of cases appear to involve some type of organized crime, even when that is broadly defined as any enduring group whose primary purpose is to generate illegal profits.[56] There are strong arguments that traditional organized crime groups, deeply penetrated into the societies in which they operate and with large investments in legitimate stocks and real estate, may have little incentive to help terrorists destabilize their home societies or to engage in nuclear activities that are likely to bring the full fury of their home states down upon them.

On the other hand, there are reasons to suspect that the role of organized crime may be larger—or may become larger in the future—than these statistics and arguments suggest.[57] First, there may be a selection bias in the public record: it may be that the known cases have little involvement of organized crime because the thieves and smugglers who *are* associated with organized crime are less amateurish and do not get caught. Second, there are cases that suggest a linkage. In the early 1990s, for example, there was a case involving tons of HEU-contaminated beryllium that were smuggled from Russia to Lithuania, which clearly involved organized crime.[58] Similarly, a low-enriched uranium (LEU) fuel element, containing a small amount of U-235 that was stolen from a research reactor in Kinshasa, wound up in the hands of the Sicilian Mafia, where it was eventually seized in an Italian police operation.[59]

Third, organized crime's presence around nuclear facilities and along key transit routes may provide opportunities for buyers to make connections to potential nuclear thieves and to move their material without detection. Shelley

and Orttung have reported cases that they describe as involving organized crime groups paying smugglers to transport nuclear materials.[60] Established smuggling routes for other contraband and corrupted border officials may provide opportunities for would-be nuclear smugglers to cooperate with organized crime groups to move their material without detection, possibly without the organized crime groups even being aware that nuclear material is the contraband that is being smuggled. A substantial fraction of Afghan heroin, for example, is known to go through Russia en route to Europe, creating opportunities for criminal and terrorist operatives from Russia, Afghanistan, and Pakistan to build relationships and to make contacts that may contribute to undetected nuclear smuggling. Two Uzbek smugglers were arrested in Kazakhstan in 2002 with a large cache of heroin and 1.5 kilograms of uranium oxide—this is at least one case where these activities merged.[61]

Shelley and Orttung have also found indications of substantial penetration of the closed nuclear city of Ozersk by organized crime (smuggling narcotics into the city by bribing the poorly paid guards, for example). Moreover, they note that under Russian law, criminals from the city were allowed to return to the city after serving their prison time and that the number of released criminals returning to Ozersk has increased markedly.[62] Such organized crime activity in a town that houses thousands of people who have access to a facility with tens of tons of plutonium and HEU clearly poses the risk that organized crime groups could make the connections needed to get involved in nuclear theft and smuggling.

Moreover, an argument can be made that newer organized crime groups that originate in conflict zones thrive on chaos, work with terrorists, and may be less restrained in dealing with nuclear or radiological materials.[63] Indeed, in the case of both the Afghanistan-Pakistan region and Colombia, drug trafficking and other criminal activities are so closely linked with terrorism that it is difficult to define the distinction between terrorist groups and organized criminal groups. The 2008 seizure of documents that indicated that the Revolutionary Armed Forces of Columbia (FARC) was considering a deal to buy and resell uranium is troubling, as it highlights that a professional group, with established smuggling operations, was potentially interested in engaging in nuclear smuggling.[64] At the same time, the documents also highlight the amateurish nature of so many nuclear smuggling cases, as the seized memorandum describes without question a $2.5 million-per-kilogram price for what turned out to be depleted uranium (a material that is essentially useless for either nuclear weapons or radiological "dirty bombs" and can readily be purchased for prices 10,000 times less).[65]

In short, the evidence available to date suggests (though it does not prove) that organized crime's involvement in nuclear smuggling has been limited. But it also provides grounds for being concerned that this restricted involvement may change in the future.

Countering the Proliferation-Corruption Linkage

Given this history, the obvious question is what steps would be most effective in reducing the dangers that are posed by corrupt individuals who participate in proliferation. Klitgaard has famously argued that corruption equals monopoly power plus discretion in using this power, minus accountability: C=M+D-A. According to this model, the obvious recommendations to control corruption are to decrease monopoly and discretion and to increase accountability.[66] Along similar lines, Huther and Shah have outlined an economic model in which potentially corrupt individuals rationally calculate the likely benefits from corruption and the probability and consequences of being caught, and are corrupt whenever the expected benefits are greater than the expected costs.[67] The obvious recommendations, using this model, are approaches that reduce the income that can be earned through bribes and increase both the probability of being caught or the penalties for being caught. But other scholars argue that a broader approach is needed, taking into account moral perceptions about corruption, differences in national cultures, and how deeply corruption has penetrated into a particular national system; the history of successes and failures in combating corruption suggests that what may work in one context may not work as well in another.[68]

Elements of the history that I have described suggest that at least some aspects of proliferation-related corruption may be different from other corruption, and may require a different response. While the states that have sought nuclear weapons in the last fifteen years—North Korea, Iran, Iraq, Libya, and possibly Syria—are all among the world's most corrupt countries, a large fraction of the corrupt suppliers of these efforts came from some of the world's *least* corrupt countries—such as Germany, Switzerland, Britain, and the United States. Hence, programs to reduce overall corruption in a particular country, by themselves, may do little to reduce the risk of proliferation-related corruption. This situation can be explained in part by the weakness of commonly perceived norms against proliferation in these countries (especially those in Europe) in the 1970s and 1980s, when many of the key technology suppliers first began to participate. At that time, the understanding that the spread of nuclear weapons was a deadly threat to the international community

was not nearly as widespread as it is in the twenty-first century; export control laws in Europe were weak and poorly enforced, European governments were actively promoting high-technology exports, and they were seeking to smooth away obstacles to such job-generating activities. Many of the participants in these networks appear to have convinced themselves that there was little harm in what they were doing, little chance of being caught, and that if they were caught, there was little chance of serious consequences. To reduce the risks of corrupt participation in proliferation networks in the future, all of these perceptions must be changed.

The pervasive secrecy that surrounds the technologies and materials of nuclear, chemical, and biological weapons makes the usual anti-corruption prescriptions of greater public openness, transparency, and freedom of information far more difficult to implement in the case of proliferation-related corruption. Another common prescription—reducing the discretion available to officials—is also not generally appropriate in this case, as all those involved in guarding nuclear, chemical, and biological stockpiles, or in stopping proliferation conspiracies, must be creative in responding to unexpected circumstances and not only use their rule-books.

To counter the proliferation-corruption linkage, I suggest a multi-pronged strategy that is based on strengthening non-proliferation norms in key sectors; improving controls over sensitive technologies; increasing the probability that proliferation-related conspirators will be caught; increasing the expected consequences of being caught for proliferation-related corruption; making it difficult to overcome proliferation controls without a large and complex corrupt conspiracy; and establishing targeted anti-corruption programs in key sectors.

Strengthening Non-Proliferation Norms in Key Sectors

Studies of compliance with safety rules indicate that the probability of compliance with a rule is high among staff who believe that the rule is important, even if there is a low probability that non-compliance will be detected.[69] Much the same is likely to be true for proliferation-related corruption. Indeed, it seems likely that the critical reason why so little nuclear theft occurred in the former Soviet Union in the mid-1990s, when security for nuclear stockpiles was alarmingly weak and nuclear workers were desperate for additional income to feed their families, was the intense patriotism and devotion to duty of the vast majority of former Soviet nuclear workers.[70] By contrast, the corrupt participants in the Khan network overwhelmingly convinced themselves that the consequences of what they were doing were either

minor or positive—that deterrence would be served by more countries having nuclear weapons or that if they did not sell these technologies others would.[71] Convincing the staff who might be corrupted at key points in the proliferation chain—and particularly those with the access to sensitive technologies and materials required to initiate such a transfer—that proliferation is a critical danger to their countries and to the world could make a substantial difference in reducing the danger of proliferation-related corruption.

In this respect, proliferation-related corruption may be far easier to counter than other forms of corruption. Even in countries where the national culture condones widespread corruption, there is generally a strong moral norm against helping other countries (or worse yet, terrorist groups) get nuclear, chemical, or biological weapons—and this culture can be built upon. This norm is strong in Russia and the other states of the former Soviet Union.

The following steps should be taken to strengthen non-proliferation norms in key sectors.

Required Training on the Proliferation Threat

Governments should: a) identify all individuals who have access to and knowledge of proliferation-sensitive technologies and materials, and b) require these individuals to participate in at least yearly briefings on the danger of proliferation, the impact proliferation could have on their country or firm, the reality of ongoing black-market attempts to acquire these technologies, the penalties for participating in proliferation, and cases where corrupt participants suffered severe punishments for their participation. At facilities with plutonium or HEU, these briefings should include not only individuals with direct access to the material but guards and others who have enough knowledge of the security system to help thieves to overcome it. At the same time, it is crucial to carry out such training in ways that do not give insiders new ideas for corrupt sales. Some of the nuclear material thieves of the 1990s, for example, were motivated by press reports of the large sums that buyers were willing to pay for potential nuclear bomb material.[72] Governments should regularly assess the effects of these training programs on targeted staff's proliferation attitudes and adjust the training approaches accordingly.

Programs to Strengthen Security Culture

Governments should require each firm or institute working with proliferation-sensitive technologies or materials to establish a program to promote a strong security culture among its staff, focused on a clear understanding of the threat, on knowledge of and willingness to comply with the security rules, and

on an understanding of the need to keep an eye out for and be willing to report on suspicious incidents and activities.[73] The United States and Russia have undertaken a joint effort to promote a security culture at Russian sites with plutonium and HEU, but there is a great deal more to be done at these sites and elsewhere around the world. The series of incidents that have taken place at Los Alamos over the decades, and the 2007 incidents in the U.S. Air Force, which led Secretary of Defense Robert Gates to ask for the resignation of both the secretary of the Air Force and the Air Force chief of staff, make clear that further steps to strengthen nuclear security culture are needed in the United States as well.[74] Finding ways to change ingrained cultures at a wide range of nuclear-related institutions throughout the world remains an extraordinary policy challenge.[75]

Building Non-Proliferation Professional Norms

An understanding of the threat posed by the proliferation of nuclear, biological, and chemical weapons, and the personal responsibility of each person who has access to technologies that are relevant to such weapons, should become a normal part of training and professional development in these fields. Professional societies should include non-proliferation pledges in their codes of ethics and professional behavior.

Improving Controls over Proliferation-Sensitive Technologies

One of the most troubling aspects of either the nuclear theft cases of the 1990s or the history of the black-market nuclear technology networks is how weak the controls were that the conspirators had to overcome. In one case in 1993, for example, an individual walked through a gaping hole in a fence at a naval base, walked to a small shed, snapped the padlock with a metal bar, entered the shed, took several kilograms of enriched uranium, and retraced his steps, without setting off an alarm or encountering a guard. No one noticed until hours later—and then only because he had been careless and had left the door of the shed partly open and the broken padlock lying in the snow. The Russian military prosecutor in the case concluded that "potatoes were guarded better."[76]

Clearly, such vulnerabilities should not be allowed to exist. Governments must put in place effective, worldwide controls over proliferation-sensitive technologies and materials. Fortunately, substantial steps in this direction have already been taken. Security for nuclear weapons, plutonium, and HEU in the former Soviet Union has improved dramatically in the last fifteen years,

and nuclear security upgrades have been undertaken in many other countries since the 9/11 attacks. After the proliferation leakage of the 1970s and 1980s, many countries in Europe and elsewhere have greatly strengthened their export control systems.

In 2004, partly in response to the Khan network, the UN Security Council unanimously approved UN Security Council Resolution 1540, which legally obligates every UN member state to "take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery," including "appropriate effective" security and accounting for any such stockpiles that they may have; "appropriate effective" border controls and law enforcement to prevent "illicit trafficking and brokering of such items;" and "appropriate effective" export controls, transshipment controls, and controls on financing such transactions, with appropriate penalties for violations. UNSC 1540 also requires every member state to adopt and enforce "effective" laws that prohibit non-state acquisition of nuclear, chemical, or biological weapons and any efforts to assist non-state actors in obtaining such weapons.[77] Unfortunately, most states have taken few, if any, actions to meet their UNSC 1540 obligations, and the major powers have taken only the most modest actions to make use of this new non-proliferation tool. Most of the steps that need to be taken to improve controls over proliferation-sensitive technologies around the world can be seen as simply implementation of states' existing UNSC 1540 obligations.

The following steps should be taken to strengthen controls over proliferation-sensitive technologies.

Establishing Effective Security and Accounting Worldwide

All nuclear weapons and weapons-usable nuclear material worldwide should be secured to standards that are sufficient to defeat the threats that terrorists and criminals can pose, in ways that will work, and in ways that will last. There is no doubt that such stockpiles must be protected against theft by corrupt insiders, as well as by outsiders with insider assistance. In particular, effective global standards for nuclear security are urgently needed; since UNSC 1540 already requires all states to provide "appropriate effective" security, the United States and other leading nuclear powers should seek to define the essential elements of an appropriate, effective system and work to help (and to pressure) all countries with nuclear stockpiles to put those essential elements in place.[78] As part of this global nuclear security effort, the number of locations where such materials exist and the scale of transport of them should be drastically reduced, making it possible to achieve higher security at

a lower cost. The nuclear material needed for a bomb is small and difficult to find; security measures to prevent such materials from being stolen are critical, as all subsequent layers of defense are variations on looking for needles in haystacks. While substantial progress in improving nuclear security has already been made, there is a wide range of additional steps that still need to be taken to achieve effective and lasting nuclear security worldwide.[79]

Improving Protection against Insider Theft

Given the corruption problem—and other means by which those seeking nuclear bomb material might convince insiders to help them—improved security against insider thieves is particularly important. Governments should ensure that no one is allowed access to nuclear weapons, separated plutonium, HEU, or information about how these materials are guarded, without a thorough background check and ongoing monitoring for indicators of suspicious activity. The number of people who have access to such materials should be kept to an absolute minimum. Such weapons and materials should be stored in high-security bunkers or vaults whenever they are not in use; access to such bunkers and vaults should only be possible for a small number of carefully screened individuals. The "two-person rule" or "three-person rule" should be maintained, so that no one is ever alone with such items.[80] Areas where such materials are processed should be continuously monitored by guards or security cameras. All windows, ventilation shafts, and other means to get such materials out of the buildings, without going through the monitored exits, should be blocked, and those blocks should be regularly inspected. Monitored exits should include radiation detectors that will set off an alarm if anyone were carrying out plutonium or HEU.

Rigorous nuclear material accounting and control systems should be put in place that would ensure that any theft of nuclear material would be detected quickly (or while it was still in progress) and localized to the area where it occurred. Regular "red team" exercises should be conducted, with insiders pretending to be nuclear material thieves, to test whether intelligent insider adversaries can find vulnerabilities in the security system. Governments should reconsider existing policies that require facilities only to be able to protect against a single insider, rather than an insider conspiracy; a substantial fraction of thefts of valuable non-nuclear items from guarded facilities around the world are perpetrated by groups that include more than one insider.[81]

Effective, Worldwide Border, Export, and Transshipment Controls

These levels of control will never be as effective as security measures at the source can be, and putting these types of controls into place worldwide will

pose even greater challenges than those posed by securing global nuclear stockpiles against theft. Leading nuclear technology states typically have put in place stronger export controls after experiences with the Iraqi and Pakistani procurement networks. But few countries can claim that they already have in place genuinely effective controls at all of their borders, on any attempts at illicit exports of proliferation-sensitive technologies, and on the transshipment of sensitive technologies through their countries. Although UNSC 1540 creates a binding legal obligation for more than 190 member states, and the Khan network had key nodes in states no one had worried would contribute to nuclear proliferation (such as Malaysia and Dubai), donor states that help countries improve their export and border controls, such as the United States, still have programs focused on only a fraction of the world's countries. Nevertheless, for the countries on which they have focused, efforts such as DOE's International Export Control Cooperation program and the U.S. State Department's Export Control and Border Security (EXBS) program have contributed substantially to improved export controls; similar efforts should be undertaken for more states. Here, too, an international effort is needed to lay out the essential elements of appropriate effective systems in each of these areas and work to help (and to pressure) states to put those essential elements in place. In the nuclear area, states should give the International Atomic Energy Agency (IAEA) the mandate and resources to help to develop interpretations of the particular steps that are required to meet the UNSC 1540 obligations, to review states' performance, and to coordinate assistance to states.[82]

Strengthening Industry Education and Internal Compliance Programs

Governments must ensure that each firm or institute with proliferation-sensitive technology fully understands existing export control laws, proliferation threats, proliferators' use of front companies and false end-use declarations, and the like. Each firm or institute with proliferation-sensitive technology should establish an in-depth internal compliance program to review not only the legality but the wisdom of proposed exports. Governments should approve legislation that makes it possible to hold a designated officer at each firm or institute personally accountable for that organization's exports—providing a strong incentive to ensure that the organization complies with relevant laws. But governments should seek to help firms and institutes carry out these responsibilities, focusing more on a partnership than on an adversarial approach. Such partnerships should include steps to encourage firms and institutes to provide information to governments about suspicious inquiries, companies that may be operating as fronts for proliferators, and the like without fear of negative consequences, and steps to encourage government

officials to provide any information and assistance that may help firms and institutes improve their internal compliance programs. Governments or industry associations should help to share the best practices of those firms that have established exemplary internal review programs.[83]

Reducing the Risks Posed by Retired Individuals with Sensitive Knowledge

From Bruno Stemmler to Gotthard Lerch and beyond, many of the corrupt participants in recent proliferation conspiracies had left the firms or institutes where they had originally received access to sensitive knowledge. Little attention has been given to the proliferation risks posed by such individuals outside the officially sanctioned system of controls. Improving controls at established firms and institutes will not solve the problem posed by people who are no longer at those places. Retired experts may pose particular proliferation risks, as they have time available and may be more vulnerable to economic desperation. Governments should establish lists of *all* individuals that have been granted access to particular areas of nuclear, chemical, and biological weapons technologies, whether they are still working in officially sanctioned firms and institutes or not, and should regularly monitor their current location and status—even after their formal clearances have expired. Pension programs should be designed to ensure that people who have particularly sensitive knowledge have enough to subsist without becoming financially desperate. Programs should be established to provide non-proliferation briefings to these individuals, and to attempt to draw them into the broader scientific community and its norms. Scientist redirection programs could be broadened to include retired individuals, for example, by providing tax reductions to firms that hire anyone who was a weapons scientist in the past.

Making the Conspiracies Needed for Success More Complex

The danger of corruption is reduced when more people at more separate locations have to participate for the corrupt act to succeed. If a single paid-off guard is enough, the risk is high, but if three or four guards in different parts of a facility would have to participate for a theft to succeed, the risk is far lower.

Steps that should be taken to raise the barriers to proliferation-related conspiracies include:

Requiring the "Two-Person" or "Three-person" Rule

Making sure that no one is ever alone with a nuclear weapon or the materials to make one is an important first rule that countries such as the United States and Russia have had in place for many years. In a discussion in 2005, I

asked a retired Russian officer who had been a senior commander of the 12th Main Directorate of the Ministry of Defense, the force that guards Russia's nuclear weapons, whether he was worried that the endemic corruption and theft in the Russian military would penetrate into that force. This provoked the blackest of humor: pointing out that the 12th maintains the two- or three-person rule, he smiled and said that as a result, most generals prefer to work with conventional weapons, where there are more opportunities to make money. Simple technological options—such as locks that require two people to turn their keys or type in their codes at the same time, several meters apart from each other, to gain access to a vault or bunker—can help enforce the two- or three-person rule and should be used.

Ensuring that Radiation Detectors Are Monitored at More Than One Location

There is always a possibility that a guard, who observes a radiation detector at some remote border crossing, or at the exit of a nuclear facility, would look the other way when the alarm goes off, or turn off the detector, in return for a bribe. Hence, to the extent practicable, all such detectors should be rigged so that both alarms and the functioning of the machine are monitored not only by an on-site guard, but by someone else some distance away as well, making it much more difficult to bribe both watchers. The U.S.-sponsored "Second Line of Defense" program, for example, helps countries install radiation-detection equipment at key ports and border crossings and often rigs these systems so that they will be monitored not only by on-site personnel but also by others off-site, such as at a regional headquarters. As of early 2006, however, the program had not yet obtained the funding that is needed to incorporate this approach consistently, wherever its radiation detectors were to be installed.[84]

Remotely Observing Personnel at Key Locations

To ensure that the systems for nuclear material protection, control, and accounting (MPC&A) that are put in place with U.S. assistance are being used appropriately and maintained, the United States and Russia have established the MPC&A Operations Monitoring (MOM) project, in which security cameras observe key locations at a few selected facilities—such as the guards at the point where staff pass through radiation detectors when exiting the facility—and transmit these images to officials elsewhere (such as to the site's security managers).[85] This approach helps to detect and deter corrupt behavior at these key points and should be adopted more broadly at nuclear facilities worldwide.

Increasing the Probability of Being Caught

Clearly, that the Khan network operated successfully for some twenty years, with scores of participants (individuals and firms) in some twenty countries, illustrates that the probability that corrupt proliferators will be caught has been too low to deter them.

In addition to the improved controls over sensitive technologies described above, several other measures should be taken to increase the probability that nuclear smuggling or black-market nuclear networks will be detected.

Expanding International Police and Intelligence Cooperation

Efforts to stop corrupt proliferation rings must be every bit as global, intelligent, and adaptive as the rings themselves. The disruption of much of the Khan network involved successful cooperation between intelligence and police agencies in several countries, particularly the United States and Britain. Governments should substantially expand the cooperation between law enforcement and intelligence agencies that are focused on nuclear smuggling and black-market nuclear technology networks.[86] This effort should include cooperative, in-depth analyses of international black-market nuclear technology networks and nuclear smuggling rings, looking at particular cases, the motivations and methods of the participants, the possible interconnections between these networks (or between these networks and organized crime or terrorist groups), and how links are forged.[87] This international cooperation should also run additional stings and scams 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. Furthermore, these efforts should be well-publicized to increase fears of such operations among potential buyers and sellers. Intelligence agents from the United States and other leading nations should also work with the semi-feudal chieftains who control some of the world's most dangerous and heavily smuggled borders to convince them to let their contacts know if anyone tries to move nuclear contraband through their domains.[88]

Strengthening Police and Intelligence Agencies' Ability to Monitor Proliferation-Related Trafficking in Key Countries

In many countries, police and intelligence agencies have little ability to understand, for example, that the precision-machined parts that are made at a particular factory in their country are for another country's uranium enrichment centrifuges. Through programs such as the International

Counterproliferation Program (ICP) at the U.S. Department of Defense, the United States and other donor countries have been providing proliferation-related training to law enforcement and border control officials in a number of countries. But there is much more to be done to strengthen police and intelligence capabilities to counter proliferation around the world. At a minimum, 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.

Establishing Well-Publicized Incentives to Inform on Proliferation Conspiracies

Most of the confirmed cases in which stolen weapons-usable nuclear material was successfully seized, or black-market nuclear technology transfers were successfully interdicted, involved having one of the conspirators or someone whom they tried to involve in the effort inform on the others. The success in convincing Urs Tinner to inform, for example, was crucial to the success in disrupting the Khan network.[89] Additional steps should be taken to make such informing more likely—including anonymous hotlines or websites that are well-publicized in the nuclear community, and rewards for credible information.

Systems-Level Approaches to Interdicting Nuclear Smuggling

The United States and other countries have invested a great deal of money to install radiation detectors at key ports and border crossings around the world. Such detectors have a real, but limited, role to play in reducing the risk of nuclear terrorism. The length of national borders, the diversity of means of transport, the vast scale of legitimate traffic across these borders, the small size of the materials needed for a nuclear bomb, and the ease of shielding the radiation from plutonium or especially from HEU all operate in favor of the terrorists. Neither the detectors now being put in place nor the Advanced Spectroscopic Portals planned for the future can offer much chance of detecting and identifying HEU metal with modest shielding—though they likely would be effective in detecting plutonium or strong gamma emitters such as Cs-137 that might be used in a so-called "dirty bomb."[90] Few of the past successes in seizing stolen nuclear material have come from radiation detectors; indeed, in many cases it is more likely that traditional counterterrorism approaches and border controls will detect the smugglers than that detectors will detect the nuclear material that they are smuggling. To gain the maximum

benefit from investments in the prevention of nuclear smuggling requires a systems-level approach that looks not just at how well an individual detector may perform but at what options adversaries have to defeat the system—by choosing other routes, bribing officials to get past detectors, hiding nuclear material in difficult-to-search cargoes, etc.—and what options the defense might have for countering those adversary tactics.[91] Extensive "red teaming" should be used to ensure that a wide range of ideas that intelligent adversaries could pursue have been explored. Based on such an analysis, the United States and other leading governments should develop a strategic plan that goes well beyond detection at borders; detailing what police, border, customs, and intelligence entities in which countries should have what capabilities by when; and what resources will be used to achieve those objectives.

Interdicting Other Elements of Nuclear Terrorist Plots

Governments should also undertake an intense international effort to stop the other elements of a nuclear plot—the recruiting, fundraising, equipment purchasing, and more that would be required. Because of the complexity of a nuclear effort, these efforts would offer a bigger and more detectable profile than many other terrorist conspiracies. The best chances to stop such a plot lie not in exotic new detection technologies but in a broad approach to counterterrorism—including addressing the anti-American hatred that makes recruiting and fundraising easier, and makes it more difficult for governments to cooperate with the United States.[92]

Strengthening the International Atomic Energy Agency's (IAEA) Efforts

The IAEA has established a small unit to collect and analyze information on black-market nuclear technology networks.[93] Among other activities, this unit, known as the Nuclear Trade and Technology Analysis (TTA) unit, has established relationships with many companies that have key centrifuge-related technologies, and has convinced them to provide information on any suspicious inquiries that they receive. But this group has few staff, little money, and little authority. Moreover, to date the purpose of this analysis is only to support the IAEA's safeguard assessments of countries' nuclear programs by providing information on what they may be shopping for; ideally, such information should also be used to warn countries and companies about potential illicit front companies and networks and to help to plug leaks. Governments should give the IAEA the resources, authorities, information, and expanded mission necessary to maximize this group's effectiveness. Governments should also consider establishing similar groups focused on chemical, biological, and missile technologies.

Increasing the Expected Consequences

Many of the corrupt participants in black-market technology networks or nuclear smuggling have received remarkably light punishments. Yuri Smirnov, who stole 1.5 kilograms of weapons-grade HEU in 1992, in the first well-documented case of theft of weapons-usable material, received three years of probation—hardly a sentence likely to deter other nuclear thieves.[94] Stemmler, a key contributor to Iraq's centrifuge program, died of natural causes without being convicted. Schaab, another notorious participant in Iraq's centrifuge program, was convicted of exporting centrifuge rotors without a license and received a fine of DM 20,000 and a suspended sentence. Later, when the full extent of his activities became clear, Schaab was convicted of treason and received a fine of DM 80,000 and a five-year term, but because he was cooperating with the German authorities and had been in jail pending trial, he was released as soon as he was convicted.[95] The British government dropped charges against Griffin, one of the Khan network's key suppliers.[96] Khan, as noted above, was under only house arrest, and was released in early 2009.

Part of the problem is that the laws that relate to such crimes in many countries are weak. Remarkably, under Article 226 of the Russian criminal code, the penalty for stealing an assembled nuclear weapon is only five to ten years. The penalty for smuggling weapons of mass destruction is the same as the penalty for smuggling drugs: three to seven years.[97] In either case, however, the Russian authorities are also able to use treason statutes, for which the penalties are more severe. Many countries have laws with even lower penalties—or may not even have laws that prohibit various types of proliferation-sensitive exports, or *attempts* to carry out nuclear theft or proliferation-sensitive exports.

Given the scale of the potential consequences, all countries should put in place laws that make real or attempted theft; smuggling; or unauthorized possession of nuclear weapons, plutonium, or HEU (or chemical or biological weapons) crimes with penalties comparable to those for murder or treason. This step would be consistent with the Convention on Physical Protection of Nuclear Material and the International Convention for the Suppression of Acts of Nuclear Terrorism, both of which require all parties to pass "appropriate penalties" for nuclear theft and related crimes, taking into account their "grave nature." Stiff penalties should also be put in place for those who participate in black-market proliferation networks. At the same time, care should also be taken to avoid a perverse effect—in which people refuse to report such crimes, or juries refuse to convict, because of a perception that the penalties are disproportionate.[98]

Ultimately, consciously helping terrorists or proliferating states obtain nuclear, chemical, or biological weapons—or attempting to do so—should be considered an international crime with universal jurisdiction (meaning that a perpetrator could be prosecuted wherever he or she were caught), similar to piracy or hijacking.[99] The first steps in this direction are already being taken. The Convention on the Physical Protection of Nuclear Material and the nuclear terrorism convention both require all parties to put in place laws under which they either take jurisdiction to prosecute offenders caught on their territory (even if the crime had been committed elsewhere and the offenders were from another state) or to extradite them. But it is not clear how many countries have in fact passed laws that give them criminal jurisdiction if a nuclear thief, smuggler, or would-be nuclear terrorist from elsewhere were apprehended on their territory. Much remains to be done to move toward universal jurisdiction for such crimes.

Establishing Anti-Corruption Programs in Key Sectors

There can be little doubt that a pervasive atmosphere of corruption and insider theft increases the risk for theft of nuclear weapons and materials. Although corrupt technology suppliers such as Stemmler, Schaab, and Lerch came from low-corruption countries, it also seems clear that pervasive corruption increases the risk for the corrupt sale of proliferation-sensitive technology and equipment.

Hence, in addition to the programs to build non-proliferation norms in key sectors that were described above, governments should also pursue targeted anti-corruption programs for particularly proliferation-sensitive firms, institutes, and agencies. These would certainly include all firms or institutes handling nuclear weapons, plutonium, or HEU; nuclear weapons designs and manufacturing technologies; or enrichment and reprocessing technologies. It would also include border control and customs officials, nuclear guards, and export control agencies.

The particular anti-corruption programs that will be most effective are likely to vary from one context to another.[100] Higher salaries, to reduce the need for corrupt supplementary income, are certainly needed in some countries for nuclear guards, technicians with access to plutonium and HEU, customs and border control officers, export control license reviewers, and nuclear security inspectors—though it should be kept in mind that men like Stemmler and Schaab were already well-to-do, not desperate and underpaid (and Khan still more so). A variety of approaches to accountability should be put

in place, including an independent inspector general (with access to all the needed information and facilities) for each critical agency involved in managing and controlling proliferation-sensitive technologies with the mission and resources to root out corruption and provide accountability for performance. Laws and institutions to protect and encourage whistleblowers should be established. Selling of jobs that include access to nuclear materials or technologies could be addressed through rules requiring that job openings be posted, open competitions held, and hiring decisions made by groups rather than individuals—combined with regular independent reviews of the reasons why particular candidates were hired. Governments should institute anti-corruption training programs for border control and customs forces, export control agencies, nuclear facilities, and others who might play important roles in proliferation-related corruption. All of these steps should be regularly assessed to see if they appear to be having the desired impact in changing attitudes and behavior.

Corruption among nuclear guards poses a particular problem, which must be dealt with through a thorough professionalization of these forces. In Russia, for example, nuclear weapons are guarded by the kind of force they should be guarded by—a reasonably well-paid, well-equipped, and well-trained professional force of volunteer soldiers. Most of those with access to nuclear weapons are officers. By contrast, sites with plutonium and HEU are primarily guarded by poorly paid and poorly trained conscripts with little idea of the importance of what they are guarding, among whom corruption is endemic.[101] Russia and other countries should shift to a system of well-paid, well-trained, well-equipped professional guard forces for all nuclear facilities.

Strengthening the Role of the Legislature, the Media, and Non-Governmental Organizations

In the United States and in a few other countries, investigations by the national legislature, the media, and non-governmental organizations (NGOs) have had a tremendous impact in revealing weaknesses in nuclear security, export controls, and similar measures, and putting pressure on governments to correct them.

Legislatures in every key country where proliferation-sensitive technologies exist should establish oversight committees charged with looking into the adequacy of their countries' controls, the dangers of proliferation-related corruption, and steps to address these dangers. Legislatures should insist on receiving the access to classified information necessary to pursue these questions. In

many countries, this change will be a step-by-step process; but an initial successful investigation can go a long way to establish a legislature's role in these areas. Governments and non-government experts should work to educate legislators in key countries on these critical issues.

While secrecy is an immense constraint, the media and NGOs do have important roles to play. Efforts should be made to educate reporters and to support NGOs that are focused on these issues in key countries, building a global network of concerned citizens who hold their governments accountable to stop corrupt proliferation networks.

Conclusion

Corruption is a central, unrecognized theme of the story of nuclear proliferation. Corruption has been a critical enabling element of the nuclear weapons programs in Pakistan, Iraq, Libya, and Iran. North Korea appears to have developed its plutonium production program largely with indigenous technology, but it appears that corruption likely played a central role in its uranium enrichment program, for which the technology was supplied by the Khan network. The attempts that al Qaeda and Aum Shinrikyo made to get nuclear weapons also relied on the central strategy of corrupting potential sellers and thieves.

Indeed, corrupt suppliers are essential to any state or to a subnational attempt to get nuclear weapons, unless the state or group in question can:

—Develop its needed technologies on its own;

—Convince states to decide consciously to supply them; or

—Convince individuals, firms, or institute suppliers to provide the needed technologies or materials by means other than cash.

Hence, better protection against corrupt proliferation conspiracies is central to strengthening the global effort to stem the spread of nuclear weapons. There is an urgent need to strengthen non-proliferation norms in key proliferation-sensitive sectors; improve protection for sensitive technologies from corrupt insiders; increase participants' perceptions of the probability and consequences of being caught; and combat corruption in firms, institutes, and agencies where corruption could contribute to proliferation.

None of these steps will be easy. Those who benefit from corruption will resist efforts to constrain it. Only through sustained leadership at high levels of many governments, which brings together a broad coalition of concerned parties—and a focus on the real danger that is posed by proliferation—can there be hope for success. As with other aspects of non-proliferation, the

political atmosphere in which states could be convinced to take additional action would be improved if the nuclear weapons states were seen to be negotiating in good faith toward nuclear disarmament.

Notes

1. See, for example, Transparency International, "Frequently Asked Questions About Corruption," available at www.transparency.org/news_room/faq/corruption_faq (accessed 7 September 2007).

2. See, for example, Griffin's assertion that "there's no bloody evidence" that he ever did anything illegal, a statement made after the British government dropped charges against him. See "U.K. Drops Investigation Into Khan Network Supplier," *Global Security Newswire* (14 January 2008). See also the interview with Griffin in Steve Coll, "The Atomic Emporium: Abdul Qadeer Khan and Iran's Race to Build the Bomb," *The New Yorker* (7 August 2006), available at www.newyorker.com/archive/2006/08/07/060807fa_fact_coll?currentPage=1 (accessed 14 September 2008).

3. See, for example, U.S. Export Administration Regulations, Part 772, Definitions of Terms.

4. For accounts of the Khan network, see, for example, International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks: A Net Assessment* (London, 2007); Douglas Frantz and Catherine Collins, *The Nuclear Jihadist* (New York, 2007); Adrian Levy and Catherine Scott-Clark, *Deception: Pakistan, the United States, and the Secret Trade in Nuclear Weapons* (New York, 2007); Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network* (New York, 2006).

5. See the account of this meeting in Frantz and Collins, *The Nuclear Jihadist,* 67–68.

6. For a typical account, see Ibid., 252–256.

7. For a published account of this episode, see Ibid., 253–257. I have supplemented this published account with personal discussions with Hassan Abbas, the National Accountability Bureau investigator assigned to review the dossier, who recommended against pursuing a case against Khan despite his manifest corruption. Abbas' book on Khan, the Pakistani bomb, and its proliferation is forthcoming.

8. One Iraqi intelligence document records an offer for centrifuge technology from a man who said he was representing Khan, which Iraq apparently did not have time to follow up on before the 1991 war. For a discussion of this offer and a translated copy of the Iraqi intelligence memo that reports it, see David Albright and Corey Hinderstein, "Documents Indicate A.Q. Khan Offered Nuclear Weapons Designs to Iraq in 1990: Did He Approach Other Countries?" (Washington, D.C., 4 February 2004), available at http://isisonline.org/publications/southasia/khan_memo.html (accessed 8 September 2008).

9. Khan's wife defends him in an article, pointing out that security at the Khan Research Laboratories was provided by a unit of 500–1,000 personnel commanded by a brigadier general. If the activities were not authorized, some portion of the security force would have to have been either fooled or corrupted. See Hendrina Khan, "Stabbed in the Back," *Spiegel Online International* (11 August 2008), available at www.spiegel.de/international/world/0,1518,571356,00.html (accessed 7 September 2008).

10. Hassan Abbas (personal communication, December 2007 and January 2009).

11. For a discussion of state capture that is focused on former communist countries, see Joel S. Hellman, Geraint Jones, Daniel Kaufmann, and Mark Schankerman, "Measuring Governance, Corruption, and State Capture: How Firms and Bureaucrats Shape the Business Environment in Transition Economies," *Policy Research Working Paper* 2312 (Washington, D.C., April 2000).

12. Frantz and Collins, *The Nuclear Jihadist,* 156–161.

13. Raymond Bonner and Wayne Arnold, "'Business as Usual' at Plant That Tenet Says Was Shut," *New York Times* (7 February 2004).

14. Syria's recent covert construction of a plutonium production reactor is an important exception. For a discussion of the concealment strategies Syria used, see David Albright and Paul Brannan, "The Al Kibar Reactor: Extraordinary Camouflage, Troubling Implications" (Washington, D.C., 12 May 2008), available at www.isis-online.org/publications/syria/SyriaReactorReport_12May2008.pdf (accessed 7 September 2008).

15. See, for example, Matthew Bunn and Anthony Wier, "Terrorist Nuclear Weapon Construction: How Difficult?" *Annals of the American Academy of Political and Social Science,* DCVII (2006), 133–149. Aum Shinrikyo, however, failed to recognize the difficulty of enriching uranium, and at one stage purchased a sheep farm in Australia and stole documents related to laser isotope enrichment—probably the most technologically demanding method for enriching uranium that was ever devised—with the idea that they would mine their own uranium and enrich it themselves to make a bomb. This effort, in essence, conforms to the common pre-9/11 prediction that people who want to commit murder on a nuclear scale are too confused in their thinking to succeed in doing so. See 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, MA, 2005), available at www.nti.org/e_research/cnwm/threat/demand.asp (accessed 14 September 2008).

16. Bunn and Wier, "Terrorist Nuclear Weapon Construction," 133–149.

17. Bunn and Wier, "The Demand for Black Market Fissile Material," available at www.nti.org/e_research/cnwm/threat/demand.asp (accessed 27 February 2009).

18. Ibid.

19. 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., 1995), available at www.fas.org/irp/congress/1995_rpt/aum/index.html (accessed 14 September 2008). For an overview of Aum Shinrikyo's nuclear efforts, see Bunn and Wier, "The Demand for Black Market Fissile Material."

20. For an account of Stemmler's role, see, for example, Mahdi Obeidi and Kurt Pitzer, *The Bomb in My Garden: The Secrets of Saddam's Nuclear Mastermind* (Hoboken, 2004), 90–92. See also "Iraq's Acquisition of Gas Centrifuge Technology: Part I: H+H Metalform—Funnel for the Iraqi Gas Centrifuge Program" (Washington, D.C., 2003), available at www.exportcontrols.org/centpart1.html (accessed 8 September 2008). For a detailed discussion of Schaab's role, see "Iraq's Acquisition of Gas Centrifuge Technology: Part II: Recruitment of Karl Heinz Schaab" (Washington, D.C., 2003), available at www.exportcontrols.org/centpart2.html (accessed 8 September 2008). See also Obeidi and Pitzer, *The Bomb in My Garden,* 120–124. The "many months" assessment is from Obeidi, the leader of the Iraqi centrifuge program. The International Institute for Strategic Studies described Schaab as "the most notorious" engineer who helped Iraq's centrifuge program, and who "probably bears more responsibility for the spread of centrifuge enrichment technology than anyone outside the Khan network." International Institute for Strategic Studies, *Nuclear Black Markets,* 47–49.

21. See "Iraq's Acquisition of Gas Centrifuge Technology: Part I: H+H Metalform—Funnel for the Iraqi Gas Centrifuge Program."

22. See "Iraq's Acquisition of Gas Centrifuge Technology: Part II: Recruitment of Karl Heinz Schaab."

23. See Frantz and Collins, *The Nuclear Jihadist,* 155–156.

24. For a discussion, see "Iraq's Acquisition of Gas Centrifuge Technology: Part I."

25. See Institute for Science and International Security, "Matrix Churchill Group" (Washington, D.C., 2003), available at www.exportcontrols.org/matrixchurchill.html (accessed 8 September 2008). See also International Institute for Strategic Studies, *Nuclear Black Markets,* 46.

26. Vladimir Orlov and William C. Potter, "The Mystery of the Sunken Gyros," *Bulletin of the Atomic Scientists,* LIV (November/December 1998), available at http://cns.miis.edu/research/iraq/gyro/index.htm (accessed 14 September 2008), 34–39.

27. John P. Holdren and Matthew Bunn, "Technical Background: A Tutorial on Nuclear Weapons and Nuclear-Explosive Materials," in *Nuclear Threat Initiative Research Library: Securing the Bomb,* available at www.nti.org/e_research/cnwm/overview/technical.asp (accessed 14 September 2008).

28. Obeidi and Pitzer, *The Bomb in My Garden,* 100.

29. "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).

30. "Russia: Criminals Indicted for Selling Mercury as Weapons-Grade Plutonium," trans. U.S. Department of Commerce, *Izvestiya* (11 October 2003).

31. A summary of multiple Russian press reports can also be found in "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 (accessed 8 September 2008), 10–11.

32. George Tenet, *At the Center of the Storm: My Years at the CIA* (New York, 2007), 275–276.

33. For a discussion of the al Qaeda and Aum Shinrikyo cases, see Bunn and Wier, "The Demand for Black Market Fissile Material."

34. For a detailed account of this case, see Oleg Bukharin and William Potter, "Potatoes Were Guarded Better," *Bulletin of the Atomic Scientists,* LI (May/June 1995), 46–50.

35. Corruption is, of course, only one of the methods that nuclear thieves might use to convince insiders to participate; blackmail is also a dangerous possibility, potentially turning trustworthy insiders into co-conspirators. In Northern Ireland, for example, one bank's security system required two senior bank officers to turn keys at the same time to open the vault. A gang, apparently associated with a splinter of the Irish Republican Army, kidnapped the families of two of the bank's senior officers. The officers opened the vault and allowed the gang to make off with millions of pounds in banknotes. See Chris Moore, "Anatomy of a £26.5 Million Heist," *Sunday Life* (21 May 2006).

36. Louise Shelley and Robert Orttung, then at American University (personal communication, September 2005). For a published account of other results from this study, see Robert Orttung 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 www.csis.org/media/csis/pubs/pm_0392.pdf (accessed 14 September 2008). A more detailed account of this work has not yet been published.

37. "The President Issued a Decree To Dismiss Deputy Chairman of the MVD Department in Charge of Law and Order in Closed Territories and Sensitive Sites, Major General Sergey Shlyapuzhnikov," trans. Anatoly Dianov, *Rossiyskaya Gazeta* (2 June 2006).

38. 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,* IX (Winter 2003), available (in Russian) at www.pircenter.org/data/publications/yk4-2003.pdf (accessed 14 September 2008).

39. Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs* (Santa Monica, 1980).

40. For corruption in the Russian military, see Tor Bukkvoll, "Their Hands in the Till: Scale and Causes of Russian Military Corruption," *Armed Forces and Society,* XXXIV (2008), 259–275. For cases involving terrorism, see the discussion in Simon Saradzhyan and Nabi Abdullaev, "Disrupting Escalation of Terror in Russia to Prevent Catastrophic Attacks," *Connections* (Spring 2005).

41. Louise Shelley and Robert Orttung, then at American University (personal communication, September 2005). This was only one element of a broad range of corruption and penetration by organized crime that the researchers found at Ozersk (formerly Chelyabinsk-65). For a published account of other results from this study,

see Orttung and Shelley, *Linkages between Terrorist and Organized Crime Groups in Nuclear Smuggling.*

42. See Institute for Science and International Security, "BNL" (Washington, D.C., 2003), available at www.exportcontrols.org/bnl.html (accessed 8 September 2008).

43. See Frantz and Collins, *The Nuclear Jihadist,* 141–142; International Institute for Strategic Studies, *Nuclear Black Markets,* 30. For more on BCCI generally, see James Ring Adams and Douglas Frantz, *A Full-Service Bank: How BCCI Stole Billions Around the World* (New York, 1992).

44. Orlov and Potter, "The Mystery of the Sunken Gyros," 35.

45. U.S. Congress, Government Accountability Office (GAO), *Combating Nuclear Smuggling: Corruption, Maintenance, and Coordination Problems Challenge U.S. Efforts to Provide Radiation Detection Equipment to Other Countries,* GAO-06-311 (Washington, D.C., 2006), available at www.gao.gov/new.items/d06311.pdf (accessed 14 September 2008).

46. See Michael Bronner, "100 Grams (And Counting): Notes From the Nuclear Underworld" (Cambridge, MA, June 2008), available at http://belfercenter.ksg.harvard.edu/files/100-Grams-Final-Color.pdf (accessed 8 September 2008); Lawrence Scott Sheets, "A Smuggler's Story," *Atlantic Monthly* (April 2008).

47. Vladimir Kovalyev, "Customs Inspectors Accused of Smuggling From Finland," *Moscow Times* (22 October 2004).

48. See David Nowak, "Adamov Gets 51/2 for Stealing $30 Million," *St. Petersburg Times* (22 February 2008). Adamov's sentence was later suspended, and he was released.

49. Interview with DOE official (August 2005).

50. Interview with official who worked closely with Adamov during his time as minister of atomic energy (September 2005).

51. Interview with a Russian site expert (July 2005).

52. Based on author's participation in these discussions.

53. "An Employee of the Department of Classified Facilities of the MVD Was Arrested in Snezhinsk: What Incriminates the 'Silovic,'" trans. Jane Vayman (29 May 2008), available at www.ura.ru (accessed 8 September 2008).

54. For a brief description of al Atheer, with overhead photographs, see "Al Atheer/al-Athir" (Washington, D.C., no date), available at www.globalsecurity.org/wmd/world/iraq/al_atheer.htm (accessed 8 September 2008).

55. For example, Yuri Smirnov stole 1.5 kilograms of 90 percent enriched HEU from the Luch Production Association in Podolsk in 1992, with no plan for how he was going to sell it. Acquaintances of Smirnov's were car battery thieves and suggested that their buyer in Moscow might also be willing to buy Smirnov's HEU. Smirnov was arrested with the battery thieves when they were at the train station, waiting to go to Moscow. See the interview with Smirnov in PBS, "Frontline: Loose Nukes: Interviews"(1996), available at www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/ (accessed 14

September 2008). For an overview of the "amateurish" nature of the known incidents in recent years and the lack of organized crime involvement in most cases, see Sonia Ben Ouagrham-Gormley, "An Unrealized Nexus?: WMD-Related Trafficking, Terrorism, and Organized Crime in the Former Soviet Union," *Arms Control Today* (July/August 2007), available at www.armscontrol.org/act/2007_07-08/CoverStory.asp (accessed 8 September 2008).

56. See International Institute for Strategic Studies, "Illicit Trafficking in Radioactive Materials," in *Nuclear Black Markets,* 132–134. This chapter, largely drafted by Lyudmila Zaitseva, is as of this writing the best publicly available overview of the known data on nuclear and radiological smuggling. For an earlier account that provides excellent anecdotal descriptions of corrupt participants at various stages of nuclear smuggling, see Lyudmila Zaitseva and Kevin Hand, "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users," *American Behavioral Scientist,* XLVI (February 2003), 822–844.

57. For recent assertions that organized crime groups *are* deeply involved in nuclear and radiological trafficking, see Louise Shelley, "Trafficking in Nuclear Materials: Criminals and Terrorists," *Global Crime,* VII (August 2006), 544–560; Louise Shelley and Robert Orttung, "Criminal Acts: How Organized Crime is a Nuclear Smuggler's New Best Friend," *Bulletin of the Atomic Scientists,* LXII (September/October 2006), 22–23.

58. This shipment involved 4.4 tons of beryllium, including 140 kilograms that was contaminated with a very small amount of HEU. For a description of the organized crime role, see Tim Zimmerman and Alan Cooperman, "The Russian Connection," *US News and World Report* (23 October 1995), 56–67.

59. What the mafia would have wanted with it, given the small amount of non-weapons-usable material that it contained, remains something of a mystery. See, for example, discussion in 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, 2005), available at www.rand.org/pubs/documented_briefings/2005/RAND_DB458.sum.pdf (accessed 14 September 2008).

60. Shelley and Orttung, "Criminal Acts: How Organized Crime is a Nuclear Smuggler's New Best Friend," 22–23.

61. International Institute for Strategic Studies, *Nuclear Black Markets,* 133.

62. Orttung and Shelley, *Linkages between Terrorist and Organized Crime Groups in Nuclear Smuggling*, 161. See also Shelley, "Trafficking in Nuclear Materials," 555–556.

63. For an extended version of this argument, see Louise Shelley, "The Unholy Trinity: Transnational Crime, Corruption, and Terrorism," *Brown Journal of International Affairs,* XI (Winter/Spring 2005), 101–111.

64. For a discussion of other FARC activities, see Jessica C. Teets and Erica Chenoweth, "To Bribe or to Bomb: Do Corruption and Terrorism Go Together?" chapter 7 in this volume.

65. See, for example, Kelly Hearn, "FARC's Uranium Likely a Scam," *Washington Times* (19 March 2008).

66. Robert Klitgaard, *Controlling Corruption* (Berkeley, 1991).

67. Jeff Huther and Anwar Shah, "Anti-Corruption Policies and Programs: A Framework for Evaluation," *World Bank Policy Research Working Paper* No. 2501 (Washington, D.C., 2000).

68. See, for example, Anwar Shah and Mark Schacter, "Combating Corruption: Look Before You Leap," *Finance & Development* (December 2004), 40–43; Omar Azfar, "Disrupting Corruption," in Anwar Shah (ed.), *Performance Accountability and Disrupting Corruption* (Washington, D.C., 2007), 255–283.

69. James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, U.K., 1997), 145. In this particular study, the chance that women would violate a rule that was perceived as "compliance important, usually legally required, but chances of detection low to moderate" was only 3 percent. The probability of noncompliance was dramatically higher if either: a) compliance with the rule was perceived as "relatively unimportant" or b) the "personal benefits of violating are high and direct"—both are circumstances that seem to have applied to the corrupt European participants in the Khan network.

70. For a discussion of security for nuclear stockpiles in the former Soviet Union in the 1990s, with photographs, see Matthew Bunn, *The Next Wave: Urgently Needed New Steps to Control Warheads and Fissile Material* (Washington, D.C., 2000).

71. See, for example, the interviews in Coll, "The Atomic Emporium."

72. See, for example, interview with Yuri Smirnov in PBS, "Frontline: Loose Nukes: Interviews."

73. For a set of recommendations for the assessment and strengthening of security culture in organizations, see International Atomic Energy Agency, "Nuclear Security Culture: Implementing Guide," *Nuclear Security Series* No. 7 (Vienna, 2008). For a good account of nuclear security culture in Russia in particular, see Igor Khripunov and James Holmes (eds.), *Nuclear Security Culture: The Case of Russia* (Athens, GA, 2004).

74. A detailed account of the inadvertent movement of six nuclear weapons, along with a review of organizational issues that contributed to this incident, can be found in Defense Science Board, Permanent Task Force on Nuclear Weapons Surety, *Report on the Unauthorized Movement of Nuclear Weapons* (Washington, D.C., 2008), available at www.fas.org/nuke/guide/usa/doctrine/usaf/Minot_DSB-0208.pdf (accessed 14 September 2008). For a remarkably harsh official critique of the security culture at Los Alamos and elsewhere in the Department of Energy system, 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.,1999), available at www.fas.org/sgp/library/pfiab/ (accessed 14 September 2008).

75. Matthew Bunn, *Securing the Bomb 2008* (Cambridge, MA, 2008), 159–160, available at www.nti.org/securingthebomb (accessed 10 January 2009).

76. Bukharin and Potter, "Potatoes Were Guarded Better," 48.

77. United Nations Security Council, "Resolution 1540," S/Res/1540 (New York, 28 April 2004). Two subsequent resolutions have extended the term of the committee that

has been established to oversee implementation. For a range of documents related to UNSC 1540 and the implementation committee's work, see "1540 Committee," available at www.un.org/sc/1540/ (accessed 8 September 2008).

78. For a discussion attempting to define the nuclear security and accounting measures that are required to comply with UNSC 1540, see Matthew Bunn, "'Appropriate Effective' Nuclear Security and Accounting— What is It?" presentation to Joint Global Initiative/UNSCR 1540 Workshop on "'Appropriate Effective' Material Accounting and Physical Protection," Nashville, TN, 18 July 2008, available at http://belfercenter.ksg.harvard.edu/files/bunn-1540-appropriate-effective50.pdf (accessed 14 September 2008).

79. See Bunn, *Securing the Bomb 2008.*

80. The two-person rule is maintained for all U.S. nuclear weapons at all times. Russian officers that are associated with the 12th Main Directorate of the Ministry of Defense (known by its Russian acronym as the 12th GUMO), which is responsible for guarding Russia's nuclear weapons, report that they go further and maintain a three-person rule so that no group smaller than three people is allowed access to a nuclear weapon.

81. In the United States, for example, the Department of Energy is now spending more than $1 billion a year on security, much of which is going to improved protection against outsider attacks that might involve large numbers of adversaries with heavy armament, helicopters, shaped-charge explosives, military training, insider information on the security system, and more. But the insider threat that facilities must defend against includes only one non-violent individual. The rationale for this approach is the belief that the established process for background checks and personnel reliability monitoring will reliably prevent people, who would use violence to carry out a nuclear theft or join in a conspiracy to carry out nuclear theft, from becoming insiders in the first place. U.S. assistance with security upgrades in other countries is also typically designed only to protect against a single insider.

82. See International Institute for Strategic Studies, *Nuclear Black Markets,* 161–162.

83. The German firm Leybold-Heraeus, for example, was deeply embarrassed by the large amount of the company's technology that UN inspectors found in Iraq. The company, now known as Oerlikon Leybold Vacuum, established an in-depth internal review program for all exports that had resulted, by 2004, in the company turning down over €20 million in business. David Albright, a critic of poor export controls and company participation in illicit proliferation, has described Oerlikon's program as a model that other companies should emulate. See briefings by Ralph Wirtz of Oerlikon and Albright (as well as the briefing by Matti Tarvainen, head of the IAEA's program to track illicit nuclear trade), in *Finding Innovative Ways to Detect and Thwart Illicit Nuclear Trade,* Carnegie International Nonproliferation Conference, 25 June 2007, transcript available at www.carnegieendowment.org/events/index.cfm?fa=eventDetail&id=1029 (accessed 8 September 2008).

84. U.S. Congress, GAO, *Combating Nuclear Smuggling,* 16–18.

85. For a brief discussion of the MOM project, see U.S. Congress, GAO, *Nuclear Nonproliferation: Progress Made in Improving Security at Russian Nuclear Sites, but the Long-Term Sustainability of U.S.-Funded Security Upgrades Is Uncertain,* GAO-07-404 (Washington, D.C., 2007), 26–28, available at www.gao.gov/new.items/d07404.pdf (accessed 14 September 2008). For earlier accounts, see U.S. Department of Energy, *National Nuclear Security Administration, Strategy Document: MPC&A Operations Monitoring Project* (Washington, D.C., 2002); Kathleen N. McCann and others, "The National Nuclear Security Administration's (NNSA) Material Protection, Control, and Accounting (MPC&A) Operations Monitoring (MOM) Project," in *Proceedings of the 43rd Annual Meeting of the Institute for Nuclear Materials Management,* Orlando, Florida, 23–27 June 2002 (Northbrook, 2002).

86. For discussions arguing, similarly, for a greater emphasis on post-theft intelligence and police interventions to reduce the threat of nuclear terrorism, see, for example, Rensselaer Lee, "Nuclear Smuggling: Patterns and Responses," *Parameters: U.S. Army War College Quarterly* (Spring 2003), available at www.carlisle.army.mil/usawc/parameters/03spring/lee.pdf (accessed 14 September 2008); Rensselaer Lee, *Nuclear Smuggling and International Terrorism: Issues and Options for U.S. Policy,* RL31539 (Washington, D.C., 2002).

87. A remarkable proportion of the analysis that is done on nuclear smuggling today is done at the level of overall statistics, rather than by in-depth analysis of individual cases and their implications. For a discussion of this point, see, for example, Shelley, "Trafficking in Nuclear Materials: Criminals and Terrorists," 547.

88. Though these individuals may be highly corrupt, it may be possible to motivate them to help to stop shipments dangerous enough to motivate governments to take action that would interfere with their normal smuggling operations. See William Langewiesche, "How to Get a Nuclear Bomb," *Atlantic Monthly,* CCXCVIII (December 2006), 80–98. While many of the specific factual assertions in this article are incorrect, this suggestion makes a good deal of sense.

89. Frantz and Collins, *The Nuclear Jihadist*, 247–249.

90. See, for example, Thomas B. Cochran and Matthew G. McKinzie, "Detecting Nuclear Smuggling," *Scientific American* (March 2008).

91. See, for example, Matthew Bunn, "Designing a Multi-Layered Defense against Nuclear Terror," paper presented at The Homeland Security Advisory Council Task Force on Weapons of Mass Effect, Washington, D.C., 13 June 2005, available at http://belfercenter.ksg.harvard.edu/publication/17189/ (accessed 14 September 2008). See also Michael Levi, *On Nuclear Terrorism* (Cambridge, MA, 2007), 6–9; 87–123.

92. For a discussion of the various stages of a nuclear terrorist plot, what available information suggests about how likely each plot is to succeed, and steps that can be taken to reduce those probabilities of success, see Matthew Bunn, "A Mathematical Model of the Risk of Nuclear Terrorism," *Annals of the American Academy of Political and Social Science,* DCVII (September 2006), 103–120. For a different approach that also focuses on many elements beyond only securing nuclear stockpiles, see Levi, *On Nuclear Terrorism*.

93. For a brief overview, see Matti Tarvainen, "Procurement Outreach in Revealing Proliferation Networks," transcript available at www.carnegieendowment.org/events/index.cfm?fa=eventDetail&id=1029 (accessed 8 September 2008).

94. See, for example, William C. Potter, "Nuclear Smuggling From the Former Soviet Union," in David R. Maples and Marilyn J. Young (eds.), *Nuclear Energy and Security in the Former Soviet Union* (Boulder, 1997), 139–160.

95. For accounts of Stemmler and Schaab, see "Iraq's Acquisition of Gas Centrifuge Technology: Part I" and "Iraq's Acquisition of Gas Centrifuge Technology: Part II."

96. See "U.K. Drops Investigation Into Khan Network Supplier."

97. See *Report of the Russian Federation on the Implementation of Resolution 1540* (2004), S/AC.44/2004/(02)/14 (New York, 2004).

98. For an interesting account of how lower penalties that have a higher likelihood that they will be imposed may work better, see Azfar, "Disrupting Corruption," 256–257.

99. For an excellent discussion of the potential power of such an international criminalization approach in the case of chemical and biological weapons, see Matthew Meselson and Julian Robinson, "A Draft Convention to Prohibit Biological and Chemical Weapons under International Criminal Law," *Fletcher Forum of World Affairs,* XXVIII (Winter 2004), 57–71, available at http://fletcher.tufts.edu/forum/archives/pdfs/281pdfs/Meselson.pdf (accessed 14 September 2008).

100. See, for example, Azfar, "Disrupting Corruption."

101. Goloskokov, "Reforming MVD Troops to Guard Russian Nuclear Facilities."