David Albright, Paul Brannan, and Andrea Scheel Stricker

Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan

That countries build nuclear weapons largely on their own is a common misperception. In fact, most states have depended heavily on overseas acquisition of vital equipment, materials, and know-how to create the industrial infrastructure to build nuclear weapons, a trend that continues today. Over the next few years, several states in dangerous parts of the world, along with terrorist organizations, are expected to seek these weapons. For most of these countries and certainly for terrorists, the pathway to obtaining or improving nuclear weapons remains through illicit nuclear trade.

Governments' ability to detect and stop this dangerous trade remains limited. Illicit nuclear trade networks remain difficult to detect, and the demand for sensitive goods by proliferant states remains robust.[1] No one knows how many nuclear procurement operations, which are primarily aimed at outfitting proliferant states' nuclear programs, exist. Too often, major successes in thwarting nuclear proliferation have depended on the last line of defense—military attacks, interdictions, and specialized intelligence operations. As important as these measures are, it is risky to depend on the last line of defense for U.S. and international security.

National and international security should instead rely on the first lines of defense such as the Nuclear Non-Proliferation Treaty (NPT), domestic and international trade controls, rigorous enforcement of these controls, diplomacy, international inspections, corporate vigilance, and early detection. Yet, these

David Albright is a physicist, president of the Institute for Science and International Security (ISIS) in Washington, D.C., and author of *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York, 2010). Paul Brannan is a senior research analyst and Andrea Scheel Stricker is a research analyst at ISIS. They can be reached at albright@isis-online.org, brannan@isis-online.org, and stricker@isis-online.org respectively.

The Washington Quarterly • 33:2 pp. 85–106
DOI: 10.1080/01636601003673857

methods all failed to detect, let alone stop, the Abdul Qadeer (A.Q.) Khan network's assistance to Iran, Libya, and North Korea in the 1980s and 1990s, Pakistani nuclear experts' assistance to al Qaeda prior to the fall of the Taliban in Afghanistan in 2001, and a secret nuclear reactor project in Syria built with North Korean assistance from the late 1990s until 2007. Six years after busting the A. Q. Khan network, the existing first lines of defense are not performing any better at deterring, catching, or prosecuting traffickers. Without improving these mechanisms, the international community is certain to have more unpleasant surprises in the coming years.

Illicit nuclear trade is neither inevitable nor unstoppable, nor is it the necessary price of global business. If the international community accepts that this trade cannot be stopped, then it is indirectly accepting that more countries and groups will acquire nuclear weapons and someday use them. The United States and its international partners can act now to bolster the first line of defense against illicit nuclear trade, and prevent the further proliferation of nuclear weapons.

Who Depends on Illicit Nuclear Trade Today

Of the roughly two dozen countries that have pursued or obtained nuclear weapons during the last fifty years, almost all of them depended critically on foreign supplies.[2] These nations have sought complete nuclear facilities, subcomponents of facilities, nuclear materials, classified know-how, and manufacturing capabilities to make key nuclear components themselves. Trade controls in practice now ban legitimate suppliers from selling reprocessing and uranium enrichment plants to countries in regions of tension, but nations can still seek nuclear subcomponents and "dual-use" goods with either ostensibly civil or military purposes which enable them to build and operate such nuclear facilities. Control of dual-use goods is particularly challenging because proliferators will try to mislead suppliers into believing they are for a civilian, nonnuclear use. Increasingly, dual-use goods sought after by proliferant states are not on supplier government lists of items subject to explicit control, making these transfers more difficult to stop.[3] Iran, for example, continues to depend heavily on illicit overseas procurement for its nuclear programs. Its most visible procurement attempts center on outfitting its growing gas centrifuge program and obtaining goods that the British, French, and German intelligence services assess are being used to develop the capability to build deliverable nuclear weapons.[4]

Currently, several states with nuclear weapons, including India, North Korea, Pakistan, and perhaps China, still depend on foreign supply to maintain or improve their nuclear arsenals. Pakistan's smuggling operations date to the 1970s

and continue today. India, on one hand, seeks parts, equipment, and technology for its civilian nuclear power program, an effort facilitated by the recent U.S.-India agreement on civilian nuclear trade, while at the same time engages in illicit activities to obtain key items for its nuclear weapons program.[5] China appears self-sufficient in maintaining and improving its nuclear arsenal, but suspicions remain that it seeks classified know-how and advanced equipment from other nations to improve its nuclear forces. Israel used to conduct extensive illegal procurements for its nuclear program, but under pressure from the United States, it stopped this practice in the 1990s. Advanced industrialized countries, such as France, Russia, the United Kingdom, and the United States, do not need illicit trade to maintain their nuclear arsenals.

North Korea occupies a special place. It has long pursued items for its own nuclear program illegally, while continuing to sell nuclear items to other states. It also acts as an intermediary in procuring conventional military, missile, and nuclear items from suppliers for others. It has purchased goods in China, Japan, and European countries for Myanmar and Syria. For many years, North Korea provided key assistance to Syria in its secret quest to build a nuclear reactor. Western intelligence did not identify the reactor construction project until late 2006 or early 2007, not long before the reactor was expected to operate. Pessimistic about other alternatives for stopping Syria's move toward developing a nuclear weapons capability, Israel destroyed this reactor in September 2007. It still remains unclear whether or not Syria will attempt to build the wherewithal to produce nuclear weapons. It may seek the help of North Korea again, or even Iran. Questions have also arisen over whether Myanmar is another nuclear customer of North Korea.

> The pathway to obtaining or improving nuclear weapons remains through illicit nuclear trade.

Particularly dangerous are nuclear proliferation networks, such as the one headed by the Pakistani scientist Abdul Qadeer Khan that was exposed and rolled up in 2003 and 2004. The A.Q. Khan network demonstrated that it is possible for a shady transnational network of engineers, industrialists, and businessmen to sell turn-key nuclear weapons production facilities. At its height, this network was dispersed over three continents and involved numerous individuals and companies that knowingly or unwittingly aided its proliferation sales to Iran, Libya, North Korea, and several other countries.[6] This network rivaled legitimate suppliers in its ability to sell nuclear facilities and capabilities to states.

The A.Q. Khan network did not survive, but other transnational networks might still exist or arise in the future. The conditions that led to the network

remain: buyers with cash and people with access to classified nuclear know-how, experience at designing as well as building nuclear facilities, and trafficking skills. A developing country could save *years* in its quest for nuclear weapons by utilizing the services of such a network. For years, there has been growing suspicion that North Korean entities will fill the void and become the next A.Q. Khan network. The revelation that such entities were helping to outfit Syria's covert reactor further solidified this concern. Alarm is also growing over whether Iran, or corrupt members of its nuclear program, could proliferate in the future.

If Iran's and North Korea's nuclear ambitions remain unchecked, in direct defiance of the major powers in the UN Security Council and UN member states, the international community could face both a cascade of states seeking nuclear weapons and a severely weakened world order to stop proliferation. A range of countries may seek nuclear weapons capabilities, particularly in the Middle East and North Asia. These countries include Egypt, Saudi Arabia, Syria, and Turkey as well as Japan, South Korea, and Taiwan. If these nations seek nuclear weapons, almost all of them would likely depend heavily on overseas assistance to outfit their effort.

There is also a growing danger that terrorist groups will acquire the ability to build their own atomic bombs. Terrorists may now be able to buy detailed nuclear weapon designs from black marketers, easing their task of building crude atomic bombs. Today, their key constraint is not having access to enough nuclear explosive material. Given the sheer amount of such materials and the inadequate controls over them in many countries, that constraint is not much comfort in the long run. Lawless regions of the globe could hide efforts by terrorists to obtain nuclear weapons. In the not too distant future, hostile groups in failed or quasi-failed states in Africa or Asia might be able to import the equipment and materials to cobble together their own crude nuclear weapons.

The only barrier to becoming a nuclear power today, compared to a few decades ago, is cash. According to former Central Intelligence Agency director George Tenet, "In the current marketplace, if you have a hundred million dollars, you can be your own nuclear power."[7] With advances in technology and a wider diffusion of knowledge, that price might come down considerably. If terrorists succeed in obtaining enough nuclear explosive material, the total price of building a nuclear weapon could be just a fraction of a hundred million dollars.

Methods Used by Illicit Trade Networks

Nuclear smuggling networks have become very sophisticated over the last fifty years—they have proven adept at adapting and learning to defeat the efforts to stop them. With illicit nuclear trade so fundamental to proliferation, those

opposed to nuclear proliferation have long focused on strategies to stop it. Unfortunately, these strategies often do not succeed because of the special difficulty of stopping nuclear wannabes who devote considerable effort to undermining them. States such as Iran, North Korea, and Pakistan currently drive the current illicit nuclear procurement schemes. Their official nuclear programs, sometimes with the help of their intelligence agencies, create state-sponsored procurement networks that seek to hide the true purpose of goods and identify the most effective ways to bypass or find loopholes in export regulations.

> In fact, the problem of illicit nuclear trade appears to be growing worse.

Smuggling networks have learned that suppliers in any country, including the United States with its extensive export laws, can be tricked into selling them sensitive goods. U.S. authorities recently arrested a man in the United States for allegedly sending sensitive vacuum pump equipment manufactured or sold in the United States to Dubai, which they suspect was routed to Iran's gas centrifuge program.[8] Smuggling networks typically route their illegal procurements through countries with weak or nonexistent export controls. By using trading companies in third countries, intermediary shippers, and complex payment schemes, these networks can use any country as a transshipment point, often called a "turntable." Popular ones include the United Arab Emirates (UAE) and Malaysia, both well-known for lacking robust controls, although the UAE has recently taken steps to tighten them. Malaysia still lacks export controls. But these are not the only turntables. Recent examples include Canada, Poland, South Korea, Taiwan, and Turkey, where the goods might travel to another turntable country before being routed to the real end-user. An important concern is China, the home of many foreign high-technology companies and a growing number of domestic manufacturers of sophisticated dual-use goods. Iran and North Korea regularly exploit loopholes and weaknesses in Chinese export controls to obtain goods for their nuclear programs.

Networks use a wide variety of approaches to obtain their goods, varying from legal to illegal methods and from straightforward to highly deceptive schemes.[9] The simplest procurement scheme involves a nuclear program or one of its domestic agents making a direct order to a supplier, where the supplier believes that the end-user is a civilian, nonnuclear program. Another, more complex scheme uses a chain of one or more trading companies, possibly located in different countries, to buy goods. The original order from the nuclear program is first sent to a domestic trading company, which orders the goods through a succession of foreign trading companies, the last of which then contacts a

supplier. Sometimes the trading companies are duped; after all, the vast majority of all trading companies are legitimate and law-abiding. Some, however, are well aware that the actual end-user is a nuclear program or at least not what it appears.

In a more devious scheme, network operatives convince manufacturing companies themselves, with clearly legitimate reasons to acquire dual-use equipment or materials, to buy the goods for them, in essence acting as trading companies but without the trading companies' baggage. Networks have developed a more elaborate ruse by arranging off-shore manufacturing of nuclear components using materials, equipment, and subcomponents bought by trading companies, all the while conniving to hide the true end-user from the suppliers, trading companies, and the off-shore company. Finally, illicit trading networks have sprung up that involve more than one proliferant state in which one country's government procures items for another state, sometimes shipping goods through a turntable.

What makes these networks so difficult for suppliers or governments to detect is that they are often small and dispersed within the immense network of global business. The legitimate global market in nuclear dual-use goods is enormous. For a supplier or a government, detecting the illicit ones is a difficult endeavor.

These trafficking networks are flexible and resilient, making their elimination difficult. Overseas trading companies are expendable to proliferant states. Once a trading company serves its purpose, or is discovered by authorities, the illicit trade network can jettison it and find a new one either in the same country or elsewhere. Removing a supplier will not disrupt the network. Another strength of these networks is that they tend to grow. Networks, once established, inevitably find new partners, or nodes, in an interconnected web of buyers and sellers.

The reason that there are so many willing partners is easy to understand. New business and profits drive all companies. Working for a proliferant state's procurement network can provide both sizeable profits and steady work. And for many such businessmen, greed can assuage any nagging suspicion that they are assisting a secret nuclear weapons effort. Too often, salesmen take a don't-ask-don't-tell attitude about suspicious sales. Some even believe it is legitimate to pursue sales that could further nuclear proliferation if it lines their pockets. They disassociate themselves from the real, terrifying prospect of nuclear weapons.

Removing a network root and branch remains very difficult. It took an extraordinary effort by the United Kingdom, the United States, and International Atomic Energy Agency (IAEA) to end the A.Q. Khan network, though few of its members have been successfully prosecuted and questions still remain about its customers and the goods it provided. Even less is known about how North Korea was helping Syria build a nuclear reactor.

Proliferant states can continue seeking items for their nuclear programs from an abundance of suppliers and intermediaries available to add to their networks. Because of this, there is a general sense that export controls can never keep up; that proliferant states will always find a way to bypass controls or find another trading company or supplier willing to make the sale, and that these states will only be slowed, not stopped, by export controls in their steadfast efforts to acquire nuclear weapons.

In fact, the problem of illicit nuclear trade appears to be growing worse as technologies and capabilities proliferate. We could easily find ourselves in a far more dangerous world. With the global spread of technology and rapid growth in international trade, trafficking networks find it easier to ply their dangerous trade. It is simpler now to obtain the materials, equipment, and know-how to produce nuclear weapons than it was ten years ago, and could be simpler still ten years from now.

Many countries that are considered developing nations have recently acquired relatively sophisticated manufacturing and machine tool capabilities that can be exploited to make items for nuclear weapons. John M. McConnell, former director of national intelligence, testified before the Senate Armed Service Committee on February 27, 2007: "The time when only a few states had access to the most dangerous technologies has been over for many years. Dual-use technologies circulate easily in our globalized economy, as do the scientific personnel who design and use them."[10]

Obama has committed to make breaking up nuclear black markets one of his administration's priorities.

New suppliers are emerging in developing markets with few export controls and a culture of indifference to stopping the spread of nuclear weapons technology. In China and other parts of Asia, export controls are both weak and poorly enforced. Businesses there often do not question the buyer or the purpose of the declared end-use. Concerns continue to grow that a combination of lax export controls and an increasing ability to manufacture reliable nuclear dual-use components will make Chinese manufacturers a very popular target for illicit procurement attempts—similar to how European manufacturers outfitted aspiring nuclear weapons programs in the 1970s and 1980s.

New technologies could also emerge that would simplify the task of making nuclear explosive materials or nuclear weapons. Experts with experience in producing nuclear explosive materials and nuclear weapons are now spread throughout the world, providing a growing reservoir of expertise for building

nuclear weapons that networks can probe for assistance. More leakage of dangerous classified information about nuclear weapons and how to make them should be expected.

Special Vulnerabilities of Illicit Trade Networks

One of the vulnerabilities of illicit trade networks centers on the ordering process. Proliferation entities leave visible traces as they try to acquire nuclear and dual-use goods and services from the open market. Companies and governments can detect these traces.

One of the most visible traces is an enquiry or request for a price quote. Enquiries are communications, which are typically faxes or e-mails, from potential purchasers or third-party contacts to a supplier. These enquiries can provide an early indication of current and possible future covert illicit trade. They can reveal both state and non-state actors since they contain names of individuals and trading companies, insight into a network's *modus operandi*, the type and amount of items sought, and end-users. A military nuclear program may need to procure thousands of individual items, but will likely use far fewer trading companies to attain them.

Enquiries from smuggling networks, however, make up a tiny fraction of the total number of enquiries a supplier receives. One large European company, which covert nuclear programs have often approached, put the fraction as less than one-tenth of a percent. The small fraction of suspicious enquiries makes detecting them challenging. To increase the chance of detecting suspicious enquiries, responsible companies establish centralized trade control offices and train their personnel to spot suspicious procurement patterns.

Identifying suspicious enquiries can improve the chance of early detection of trafficking networks before an order is made or any goods are shipped. If suppliers and governments cooperate on spotting suspicious enquiries, governments can use the information gained from companies to disrupt a network's operations. For example, a European vacuum manufacturer received multiple enquiries over several months in 2002 and 2003. The first ones coincided with the public exposure of the Natanz gas centrifuge plant in the fall of 2002 and provided independent support that Iran was seeking to scale up its gas centrifuge program. The enquiries came from trading companies in Iran, Italy, and South Korea, and some European countries. Sometimes an enquiry was routed through more than one trading company.[11]

The enquiries from the European trading company could have appeared as a domestic transaction, not even involving an export since these trading companies have the ability to shield the proliferator's nuclear program from the supplier. But in this case, the supplier was alert and suspected that the

end-user was Iran's nuclear program. It ignored the enquiries and turned them over to authorities. Discretion and expertise about the company's specialized products helped the manufacturer's trade control office bring the enquiries to the attention of a European government agency, which eventually agreed that the valves could be for gas centrifuges, and alerted other companies and governments. This process, however, took over a year. In the meantime, Iran obtained the valves elsewhere from less vigilant suppliers. But this example shows how early detection, if acted upon globally, would have thwarted Iran's attempt to obtain critical goods for its enrichment program.

Similarly, in late 2006, the export control office at a large European manufacturer noticed a suspicious pattern of enquiries from trading companies in Pakistan and the UAE (mainly in Dubai) for dual-use equipment.[12] The manufacturer's export control office suspected that the items were for use in Pakistan's gas centrifuge uranium enrichment program and ignored the enquiries. This office receives and analyzes suspicious enquiries from the manufacturer's many subsidiaries and sales agents located throughout the world. It functions as a hub of its own network aimed at detecting and stopping potential illicit procurement attempts, a "detection hub" for short.

The barrier to becoming a nuclear power today is not nuclear materials, but cash.

For many years, Pakistan has recognized that its enquiries will often be met with skepticism and that suppliers will ignore many of them. As a result, its agents send out enquiries for the same items to many manufacturers, and often to several offices of the same company located in different countries, in essence using a barrage approach to procurement in order to increase its chances that one order will slip through controls. This strategy also tries to exploit any lack of communication among a single manufacturer's sales agents by sending a large number of enquiries within a short period of time, or all at once. Without a centralized export control office, the individual sales offices of a manufacturer would be unaware of the identical enquiries sent by the same trading company to other sales offices.

These examples show that this network of traffickers, suppliers, and trading companies interconnected by enquiries tends to have a structure of a few dominant nodes—or proliferation hubs—with many connections to other nodes. A large number of nodes are on the periphery with few connections.[13] Many enquiries originate from these dominant nodes or hubs. This type of network has demonstrated success in being able to secure orders from a wide range and number of suppliers throughout the world, and is difficult to disrupt.

A network of this type also has characteristics of a "small world" network, which in this case means that the supplier is not "far" from those nodes acquiring the items for a nuclear program.[14] This helps explain the importance of cooperation between governments and suppliers: these suppliers can provide governments with valuable, real-time information about traffickers and their associated trading companies, allowing governments to disrupt their activities.

These examples illustrate how Iran and Pakistan use domestic trading or civilian manufacturing companies to create overseas contacts with suppliers or intermediate trading companies. Eliminating nodes inside Iran or Pakistan is extraordinary difficult, since the state will protect the individuals working on such efforts. Even if these individuals are identified, the state is unlikely to extradite them or otherwise make them available to foreign prosecutors. An innovative approach pursued by the United States, at least in the case of Iran, is to lure these individuals overseas to friendly countries where authorities can arrest and extradite them. U.S. authorities lured Ali Hossein Ardebili, a prolific procurement agent of U.S. military equipment, to Tbilisi, Georgia, where he was arrested and later extradited to the United States and pled guilty to charges.[15] Another Iranian agent, operating from Iran, was arrested in Germany for allegedly illegally transshipping vacuum pump equipment bought in the United States.[16]

Making export control laws universal and enforcing them is necessary.

The persistence of illicit nuclear trade follows from the difficulty of stopping proliferant states from finding or establishing new trading companies abroad, which subsequently locate new suppliers willing to deliberately or inadvertently ship critical goods to a nuclear program. In the case of the A.Q. Khan network and North Korea's assistance on the Syrian reactor, the last line of defense against proliferation—namely specialized covert intelligence operations, cargo interdictions, and military strikes—worked to stop their efforts. Yet, these tools, while important, cannot be counted upon every time or even the next time. Intelligence operations, shipment interdictions, and military strikes all have serious shortcomings when used as a last resort to prevent proliferation.

The U.S. intelligence community, in cooperation with its foreign partners, works to identify, penetrate, and disrupt nuclear smuggling and proliferation networks. These operations are often successful, but they miss most transactions. Innovative interdiction approaches, such as the Proliferation Security Initiative (PSI) that calls on participant states to stop transnational trafficking operations and carry out cargo seizures of suspicious shipments crossing their territories, rely heavily on imperfect intelligence and are unable to catch most illicit shipments.

Military strikes, as a policy of preventing proliferation, can temporarily remove known nuclear facilities, but can also prompt states to take their nuclear weapons programs further underground, making them less observable to foreign intelligence agencies. The limitations of intelligence operations and interdictions show that the nonproliferation regime cannot depend wholly on these approaches to prevent illicit trade, nor can it depend on military operations to deal with its consequences.

Bolstering the First Lines of Defense

Three essential steps on the first lines of defense should be taken to prevent further proliferation: implement and enforce universal laws and norms against nuclear trafficking, establish more secure nuclear assets, and work toward earlier detection of illicit nuclear trade.

Make Export Controls Universal

Making export control laws universal and enforcing them is necessary in order to break up these illicit networks. Export or trade controls are the foundation of efforts to stop the outfitting of nuclear weapons programs. These controls are deeply embedded in the NPT and its emphasis on ensuring the peaceful use of nuclear energy. They are also at the core of efforts of the widely respected Nuclear Suppliers Group (NSG), a multinational group composed of advanced supplier states. Members of the NSG all export goods that can be used in nuclear programs and coordinate their export controls to prevent the supply of items to unauthorized uses.

Although few industries look favorably on export controls, the intention here is not to stop progress or interfere in the pursuit of business. Preventing the misuse of civilian goods in nuclear weapons programs should be a global moral imperative. And given the negative and lasting consequences faced by companies that are notorious for supplying to nuclear weapons programs in the past, it is in each individual company's interest as well.

Rigorous prosecution of major export violations is required to stop existing violators and deter future potential traffickers. This, however, is more of a goal than a reality in most parts of the world. Ineffective prosecutions of traffickers show that too often, major violators evade punishment for their acts, encouraging others to join the lucrative business.

The prosecutions of members of the A.Q. Khan network showed that successfully prosecuting transnational nuclear traffickers can be extraordinarily difficult. Export control laws varied widely and some countries, such as Malaysia and the UAE, lacked such laws at all (UAE adapted its first laws in 2007). Rules that governed transnational evidence sharing and access to foreign witness testimony differed, harming international cooperation in cases against several

The crime of illicit trade continues to receive low penalties even when violators are convicted.

members of the network. Bilateral extradition treaties failed to cover the modern crime of illicit nuclear trade, and domestic legal processes, legal definitions, and judicial attitudes toward such trade differed by country. Finally, violators themselves were often untouchable because they were located within the territories of proliferant states, as in the case of Khan and his Pakistani associates. What's more, all of these prosecutorial problems still exist today, six years since the A.Q. Khan network prosecutions began, and as a result, many prosecutions have floundered.

Compounding all of these obstacles is the fact that the crime of illicit trade continues to receive low penalties even when violators are convicted, both in terms of jail sentences and fines, compared to the enormous profits accrued from illicit trading activities. The few A.Q. Khan network smugglers convicted of a crime generally served only months to a few years in jail and few received fines large enough to deter other traffickers. To overcome these problems, domestic legal processes must be improved to more effectively try and punish trafficking. Extradition treaties and rules governing witness testimony and evidence-sharing should be revised to allow access by foreign countries to nuclear trafficking suspects, case witnesses, and needed information. Laws must be revised to allow prosecutors to more effectively garner tough sentences for traffickers. States should also agree to implement universal prosecution guidelines for prosecuting illicit nuclear trade that include commitments to aid other countries' prosecutions.

As a backup to national prosecutions, the UN Security Council should sanction major transnational nuclear traffickers. States could also agree under a UN Security Council resolution to grant universal jurisdiction to major cases of nuclear trafficking which would allow a state to prosecute noncitizens for crimes committed elsewhere, treating significant nuclear trafficking as a crime which any state is authorized to punish.

States should also develop an international organization or office responsible for coordinating transnational prosecutions of significant nuclear traffickers, a mandate which could naturally fall under the International Criminal Court at The Hague, and raise the moral significance of the most serious crimes of nuclear trafficking to the level of internationally-recognized crimes against humanity. Over time, this measure could evolve into a common international criminalization system that would more effectively deter nuclear trafficking. The transfer of the capability to develop, produce, or trade nuclear weapons deserves international censure, because acquisition of nuclear weapons severely

threatens international security and the detonation of a single nuclear weapon can kill tens or even hundreds of thousands of innocent people.

Another problem that must be solved is the fact that not all countries have export controls. The UN Security Council has already mandated that all countries should establish and implement export controls. In 2004, the UN Security Council passed resolution 1540, calling upon all states to adopt modern export control systems and implement penal codes that criminalize proliferation to non-state actors.[17] Resolution 1540 aimed to help integrate countries that are not members of the NSG into a broader, rules-based export control system. In September 2009, the UN Security Council passed resolution 1887 that in part reiterated states' obligations under 1540, calling upon states to "adopt stricter national controls for the export of sensitive goods and technologies of the nuclear fuel cycle."[18]

UN resolution 1540 requires states to develop modern financial controls to prevent proliferation financing. In developed countries, major financial institutions already employ sophisticated screening systems that flag suspicious transactions by looking for information included in transactions against a list of suspicious names, entities, and related information, allowing them to freeze or refuse transactions attempted by proliferators. Banks in developed countries are also subject to strict reporting requirements which oblige them to report any potential illegal activity that they detect to the relevant authorities. In less developed countries, such systems are often not yet in place, and for this reason their banks might be targeted by proliferation networks. Developed nations should strengthen programs to assist these countries in fulfilling obligations under resolution 1540 to create financial tracking and screening systems as well as reporting requirements which would help close global financial loopholes exploited by procurement networks.

Increased prosecution of financial violations around the world would also send a message to traffickers that their activities may pose legal risks. The United States has recently had some success in prosecuting financial transaction violations. In 2009, then New York District Attorney Robert M. Morgenthau announced a $536 million settlement with Credit Suisse and a $350 million settlement with Lloyds TSB for making transactions with U.S. financial institutions on behalf of Iranian banks.[19] His office also indicted a Chinese individual, Li Fang Wei, and his company for illegally transacting with New York banks under aliases to receive payments from Iran for illicit procurements of equipment and materials usable in missile, nuclear, and military programs. China, however, has so far refused to arrest him, let alone extradite him to face charges in the United States.[20]

Compliance with resolution 1540 continues to lag. It is unclear whether resolution 1810, passed in April 2008 to launch a comprehensive review of 1540

compliance, has succeeded thus far.[21] The 1540 committee, established to review implementation of states' obligations, stated in its July 2008 report, roughly four years after 1540 was passed, that member states "need to do far more than they have already done to implement resolution 1540."[22] Continued failures of compliance over time will contribute to proliferation and a breakdown in global security since noncompliant countries will remain important transshipment points for controlled or dual-use nuclear equipment heading to suspect countries.

In 2007, U.S. pressure succeeded in persuading the UAE to implement export controls, an effort meant to address the consistent use of that country by nuclear procurement networks as a turntable to transship goods to sensitive countries. Nonetheless, enforcement lapses still persist, particularly in Dubai. Some former transit points, such as Hong Kong and Singapore, have changed dramatically for the better. But developing nations, such as China and Malaysia who prioritize economic growth over fulfilling international mandates, continue to resist 1540 implementation. Malaysia, a former base of operation for the A.Q. Khan network, still has not created export control laws and continues to serve today as a popular turntable for the diversion of goods to the nuclear programs of Iran and Pakistan.[23]

The most significant shortcoming is the lack of systematic methods to detect nuclear trafficking.

To increase pressure on noncompliant states to abide by their nonproliferation obligations, the UN Security Council should strengthen the provisions of resolution 1540, launching a coordinated diplomatic campaign to increase compliance with the resolution, along with providing broad financial and consultative assistance to lagging countries on implementing adequate controls, legislation, and enforcement. President Barack Obama has committed to give new impetus to 1540 implementation and make breaking up nuclear black markets one of his administration's priorities.[24] Obama also will hold a global nuclear security summit in April 2010, where one of his stated intentions is to find ways to combat nuclear smuggling and urge states to implement their 1540 obligations.[25] Obama should use this major nuclear security platform to announce that failure to take action will have consequences directly related to trade. The United States as a matter of policy should state that it will consider imposing additional export licensing requirements on states that do not meet their obligations to ensure that goods are not transshipped to proliferant states—the threat of doing so was instrumental in convincing the UAE to create export control laws.

The United States should also use its full diplomatic weight to halt one of the principal causes of illicit nuclear trade—the use of trafficking networks by

nuclear-aspiring states (Iran and North Korea) and two states outside the NPT (India and Pakistan) to obtain needed wares for their nuclear weapons programs. In the case of partners like India and Pakistan, the United States should simply pressure them to stop breaking its and other nations' laws to outfit their nuclear weapons programs. Under U.S. pressure in the 1980s and early 1990s, Israel—which formerly rivaled Pakistan in the extent of its nuclear smuggling—decided to stop its illicit procurement for its nuclear weapons program. The United States should expect no less from India and Pakistan.

For countries like Iran and North Korea, negotiated agreements to limit their nuclear programs must include commitments to halt proliferation of nuclear technology and engaging in illicit trafficking. Negotiators have shied away for too long from making the achievement of verifiable commitments against illicit nuclear trade a priority. Illicit nuclear trade is often excluded from negotiations out of fear of its impact on other negotiations. Its inclusion, however, would be invaluable as an additional way to inhibit a country's ability to build secret nuclear sites and, more importantly, ease the task of verifying that these countries do not have undeclared nuclear facilities. To its credit, the Bush administration insisted that North Korea's proliferation should be part of the Six-Party Talks but hesitated to expand the discussion to include all of North Korea's illicit nuclear procurements. Likewise, any negotiations to limit Iran's nuclear program would benefit from including bans on illicit nuclear trade. A stronger and more inclusive verification agreement only builds more confidence among interested parties in the reliability of the negotiations.

Over the long term, export controls should be broadened internationally and an international verification mechanism created to ensure their effectiveness. An export control system based in both international law and standards would help to close loopholes in the existing patchwork of controls and create more effective criminalization procedures. Under such an arrangement, countries would implement a set of export controls similar in nature to those required in UN Security Council resolutions 1540 and 1887. This approach, however, would also require an organization to verify compliance, ensure the adequacy of states' laws, and investigate illicit procurement activities. Based on its experience with Iran, Libya, and the A.Q. Khan network, the IAEA is a logical choice for this verification organization. This mandate would complement its existing safeguards mission. A global export control system would provide critical assurances to the international community that countries are not pursuing nuclear weapons and act as an early warning system if a country or sub-national group seeks to build them.

Protect Nuclear Assets

Protecting nuclear assets and information against theft from nuclear weapons states is vital to preventing proliferation to states and terrorists. Illicit nuclear

We can no longer assume that detailed nuclear weapon designs are not available to proliferators.

trade networks provide a shortcut on the path to nuclear weapons if they can obtain nuclear explosive materials through theft or diversion. So far, it is unknown if networks have traded in these materials in any substantial manner, but they could do so in the future, greatly magnifying the threat. In his April 2009 speech on nuclear disarmament in Prague, Obama called for securing all vulnerable nuclear material within four years. He committed the United States to work with Russia and partner with others to dramatically improve the protection of these sensitive materials. Governments must work diligently and cooperatively to meet Obama's goal by ensuring that all fissile material facilities are secured from infiltration and attack, and that personnel with access to fissile materials follow procedures that ensure they cannot be stolen.

But protecting nuclear material is not enough—securing sensitive nuclear information and data is also vital. Without detailed gas centrifuge information and designs, few countries could successfully build a gas centrifuge plant. Nations make different, sometimes conflicting, decisions about which information is sensitive and how much to protect it. After it was revealed that India was incidentally leaking centrifuge component design drawings, through its free-for-all tender bidding process in support of its unsafeguarded uranium enrichment program, the Indian government responded that it did not consider these designs to be classified.[26] Yet, gas centrifuge design drawings in most states are indeed classified. Developing uniform international standards over sensitive nuclear information is long overdue.

The need to standardize internal controls over sensitive information is also demonstrated by Pakistan's long history of inadequate controls over its sensitive nuclear weapons information. One of Khan's most dangerous innovations was ingeniously marketing designs and manufacturing instruction booklets for centrifuges and nuclear weapons, developing packages containing key equipment and, often times, digitized documentation. He made the information more user-friendly and eased its dissemination. These instructions were sufficient to achieve the many steps in the process of building a nuclear weapon. Although the danger that such detailed designs would emerge on the Internet has not been realized, we can no longer assume that detailed nuclear weapon designs and other sensitive information are not available to proliferators or terrorists. It is imperative that responsible governments seek to recover these and other sensitive information.

Improve Detection of Illicit Trade

The single most significant shortcoming of the current system is the lack of systematic, universal methods to detect nuclear trafficking. Early detection is key to preventing illicit nuclear trade. The first step is to improve the chance of detecting secret nuclear facilities and activities in states conducting illicit nuclear trade. In this effort, an underutilized tool is the IAEA Additional Protocol to the NPT and IAEA investigatory capabilities.

One of the IAEA's central inspection tools is the Additional Protocol, developed in the mid-1990s to expand the IAEA's inspection rights and make it much easier to detect when a country has a secret nuclear facility. The protocol makes a country's nuclear program far more transparent than what is provided by older, weaker inspections arrangements. Under the protocol, the inspectors can investigate questionable imports and exports to determine whether a state is in compliance with its treaty obligations. If the IAEA learns of suspicious purchases, it can press the country for more information.

Not surprisingly, this detection tool remains largely unimplemented among countries most prone to proliferate. Iran, Syria, and prior to its leaving the NPT, North Korea, have refused to implement the Additional Protocol. The IAEA and its key member states have not insisted that countries that have signed the NPT also implement this far more powerful inspection agreement. This mistake should be reversed. Any country refusing to accept the Additional Protocol should not receive nuclear assistance from the IAEA or any other countries.

The IAEA's experienced and technically sophisticated inspectorate is unique in its ability to collect and assess information. Even intelligence agencies rarely have the technical depth of the IAEA and a sustained commitment to maintaining that level of expertise. Because of its experiences uncovering the nuclear smuggling activities of Iran, Libya, and the A.Q. Khan network, the IAEA established a special program to detect trafficking networks.[27] On a limited basis, it tracks transnational nuclear networks and non-state actors to increase its chances of detecting and responding to nuclear proliferation risks. To that end, it collects and analyzes nuclear trade information, seeking to better understand existing illicit networks and reveal unknown ones.

Nonetheless, its potential often lies dormant. A fundamental part of improving this initiative is enabling the IAEA to better collect suspicious enquiry data from high-technology manufacturers that contain key information about the goods sought and the people seeking them. The IAEA must obtain the support of the government of the country where high-technology manufacturers reside before it contacts individual companies to acquire data. It now has an outreach program to many countries. Despite supporting the initiative in general, however, the Bush administration did not give the IAEA the green light

for its effort to collect information from U.S. companies directly or through a U.S. agency. The United States should embrace the IAEA's effort.

Another method to improve illicit trade detection capabilities is to expand government-industry cooperation. Companies which export sensitive or dual-use nuclear equipment can function as a vital component of an early detection system because they are approached by traffickers in the course of doing business. Robust cooperation between governments and companies in identifying nuclear trafficking schemes needs improvement in many countries, including the United States. Companies are directly targeted by illicit procurement networks each day with enquiries for goods ultimately intended for covert nuclear weapons programs. They often spot suspicious enquiries, but typically throw them away or delete them from their computer systems. Yet, because companies do not have their own "intelligence departments," they cannot possibly identify all sophisticated trafficking attempts and sometimes unwittingly supply items to nuclear programs.

Although U.S. enforcement agencies conduct successful outreach to industry, they do not receive as much useful information as they could. In the United States, companies have greater concerns about potential prosecutions, which have been amplified in the last several years by statements by senior U.S. policy officials overemphasizing prosecutions of accidental export control lapses. U.S. companies are concerned about their exposure to penalties when cooperating and are left on their own to determine to what extent they need to protect themselves from possibly revealing unknown accidental violations.

U.S. export control agencies do publish lists of certain entities believed to be involved in proliferation activities of concern, for example on the U.S. Department of Treasury's proliferators lists and the U.S. Department of Commerce's entity list. But these lists of suspicious individuals and entities intended to help companies make responsible export decisions are often obsolete by the time they are published. New front companies replace old ones too fast for these lists to be up-to-date or helpful in detecting new trafficking schemes. Investigating a trading company suspected of illicitly procuring items can require months or even years, meanwhile allowing plenty of time for the trading company to procure items for proliferant states before it receives U.S. government sanctions or is added to entity lists viewable by suppliers. U.S. authorities have resisted providing real-time tips about particular entities involved in illicit procurement activities that may be targeting the company's products. Without that type of help, companies are unable to identify illicit trading networks by themselves and prevent them from eventually obtaining targeted goods.

There are better methods to expand cooperation. In Germany and the United Kingdom, companies regularly provide information to authorities, while their

governments tip off companies about illicit procurement networks targeting their products in order to prevent an inadvertent sale. British authorities maintain contact with more than 2,000 domestic companies, trade associations, and academic institutions through phone calls, emails, and personal visits. From them, the British government receives technical advice, enquiries and orders from entities of concern, and suspicious enquiries from unknown entities.[28] Similarly, German authorities provide companies confidential "early warning" letters that include lists of suspicious entities and strategies used by proliferant states. Companies forward suspicious enquiries to authorities on a voluntary basis. In the nuclear area, intelligence officials meet periodically with key company officials to provide tips to watch for specific illicit procurement trading companies, technical specifications, and end-users. In turn, they receive important information from the companies. Upon receiving these tips, a company may also review its recent enquiry data and report back to the authorities about any contact with these entities.

The first line of defense is not currently adequate to deter, catch, or prosecute traffickers.

Common to the British and German systems is the notion that government and industry will prevent more illicit trade by working together because they otherwise both have limited access to each other's information about illicit procurement attempts and suspicious enquiries. Companies have intimate knowledge about the underlying technologies of their products and their potential misuse, usually far better than the government's knowledge. Governments, on the other hand, have greater access to knowledge about illicit trading networks and suspicious entities. By working together, companies face less risk of inadvertent illegal exports and governments gain access to a range of invaluable information useful in stopping illicit trade domestically and internationally.

As trust built in Germany and the United Kingdom, these relationships have become critical to both countries' efforts to thwart illicit nuclear trade to sensitive countries. This cooperation has also led to an unprecedented amount of operational intelligence.[29] In a large number of cases, actions taken as a result of this intelligence lead to disruptions of exports to nuclear programs or improved company compliance. The governments also receive a significant amount of strategic intelligence about covert nuclear programs, contributing to a much deeper understanding of these programs, and providing new insights as well as key corroboration of intelligence assumptions and estimates.

A greater level of cooperation is needed in the United States. This new approach should place an emphasis on facilitating an equitable flow of

information between the U.S. government and companies. Industry would provide the government with significantly more procurement data than they do now. For its part, the U.S. government would provide tips before an enquiry turns into a sale. U.S. companies also need a systematic way to contact government officials or liaisons who could investigate whether it is advisable to make a sale to a particular foreign company. These company officials could liaison with government officials in order to check whether a firm or its agents have been associated with trafficking schemes.

Creating a Bedrock for Nonproliferation

The first line of defense is not currently adequate to deter, catch, or prosecute traffickers in dangerous nuclear goods. Ignoring this weakness risks more destabilizing, covert nuclear programs in the future. Implementing universal laws and norms against illicit nuclear trade, establishing more secure nuclear assets, and achieving earlier detection of nuclear trade are critical to stopping the spread of nuclear weapons to other states and terrorists. Few can build nuclear weapons on their own, meaning that illicit nuclear trade is here for the long term. Better understanding, detecting, and disrupting such trade must be a priority. The international community must make countering illicit nuclear trade a bedrock of international nonproliferation efforts.

Notes

1. In this article, a network is an interacting collection of companies and individuals engaged in a process of procuring capabilities to make nuclear weapons. The use of the term network is to avoid characterizing these proliferation activities as an organization and to include all aspects of the activities necessary to organize this effort, deceive suppliers, order goods, pay for them, and ship them.
2. Thomas C. Reed and Danny B. Stillman *The Nuclear Express: A Political History of the Bomb and Its Proliferation* (Minneapolis, MN: Zenith Press, 2009) and Institute for Science and International Security (ISIS), "Nuclear Weapons Programs Worldwide: An Historical Overview," Web site, n.d., http://isis-online.org/nuclear-weapons-programs/.
3. Other items not on government control lists are covered by "catch-all" controls. These controls provide a legal or regulatory basis to require government permission for exporting these unlisted items when there is reason to believe such items are intended for a missile program or for the development of weapons of mass destruction. In practice, catch-all is very hard to implement without government assistance.
4. See David Albright and Christina Walrond, "The Trials of German-Iranian Trader Mohsen Vanaki: The German Federal Intelligence Service Assesses That Iran Likely Has a Nuclear Weapons Program," December 15, 2009, http://www.isis-online.org/uploads/isis-reports/documents/MohsenCaseStudy_update_15Dec2009.pdf and multiple interviews with British, French, and German officials by ISIS staff, 2008 and 2009.

5. See David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010) and ISIS, "Illicit Trade: Case Studies," Web Site, 2009, http://isis-online.org/studies/category/illicit-trade/.
6. Albright, *Peddling Peril* and David Albright and Corey Hinderstein "Unraveling the A.Q. Khan and Future proliferation Networks," *The Washington Quarterly* 28, no. 2 (Spring 2005): 111–128 http://www.twq.wm/05spring/docs/05spring_albright.pdf.
7. George Tenet, *At the Center of the Storm*, (New York: HarpersCollins, 2007), p. 287.
8. David Albright, Paul Brannan, and Andrea Scheel Stricker, "Arrests in Scheme to Export Vacuum Pump Equipment to Iran from the United States" (Washington, D.C.: ISIS, forthcoming).
9. For more in-depth studies of these strategies, see Albright, *Peddling Peril* and "Illicit Trade: Case Studies."
10. J. Michael McConnell, director of national intelligence, statement for the record before the Senate Committee on Armed Services, February 27, 2007, http://www.dni.gov/testimonies/20070227_testimony.pdf.
11. See David Albright, Paul Brannan, and Andrea Scheel, "A Company's Discretion Detects Large Iranian Valve Orders by Scrutinizing Items and End-Users Instead of Lists," January 28, 2009, http://www.isis-online.org/uploads/isis-reports/documents/Iran_Valves_28January2009.pdf.
12. See David Albright, Paul Brannan, and Andrea Scheel, "Detecting the Barrage Approach to Illicit Procurement," January 12, 2009, http://www.isis-online.org/uploads/isis-reports/documents/PakistanBarrageApproach.pdf.
13. On a much smaller scale, this type of illicit trading network appears to have some of the characteristics of a scale-free network, For background on scale-free networks, see Mark Newman, "The Physics of Networks," *Physics Today*, November 2008, http://scitation.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=PHTOAD000061000011000033000001&idtype=cvips&prog=search&bypassSSO and Mark Newman, Albert-László Barabási, and Mark Newman, *The Structure and Dynamics of Networks* (Princeton, NJ: Princeton University Press, 2006).
14. Ibid.
15. David Albright, Paul Brannan, and Andrea Scheel Stricker, "Inventive U.S. Sting Operation Catches Iran-Based Military Equipment Smuggler," February 16, 2010, http://isis-online.org/isis-reports/detail/inventive-u.s.-sting-operation-catches-iran-based-military-equipment-struggl/.
16. Albright, Brannan, and Stricker, "Arrests in Scheme to Export Vacuum Pump Equipment to Iran from the United States."
17. See UN Security Council Resolution 1540, S/RES/1540 (2004), April 28, 2004, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/328/43/PDF/N0432843.pdf?OpenElement.
18. UN Security Council Resolution 1887, SC/9746, September 24, 2009, http://www.un.org/News/Press/docs/2009/sc9746.doc.htm.
19. See Joshua Gallu, Karen Freifeld, and Cary O'Reilly, "Credit Suisse to Pay $536 Million in U.S. Settlement," Bloomberg.com, December 16, 2009, http://www.bloomberg.com/apps/news?pid=20601103&sid=aG1wyIpbsqCU and Karen Freifeld, "Lloyds TSB to Pay $350 Million to Settle Probe," Bloomberg.com, January 10, 2009, http://www.bloomberg.com/apps/news?pid=20601103&sid=aeBCUImC3lMk.
20. Andrea Scheel Stricker, "A Smuggler's Use of the U.S. Financial System to Receive Illegal Payments from Iran," October 23, 2009, http://www.isis-online.org/uploads/isis-reports/documents/Limmt_Li_Fang_Wei_23Oct2009.pdf.

21. See UN Security Council Resolution 1810, SC/9310, April 25, 2008, http://www.un.org/News/Press/docs/2008/sc9310.doc.htm.
22. UN Security Council, letter dated July 8, 2008 from the chairman of the Security Council Subcommittee established pursuant to resolution 1540 (2004), addressed to the president of the UN Security Council, July 30, 2008. pp. 22–25.
23. Justin Blum, "Iran Gains U.S. Military Technology Through Malaysia Middlemen," Bloomberg.com, September 14, 2009, http://www.bloomberg.com/apps/news?pid=20601087&sid=aK4daf8MD.Bw.
24. The White House, Office of the Press Secretary, "Joint Statement by President Dmitriy Medvedev of the Russian Federation and President Barack Obama of the United States of America," April 1, 2009, http://www.whitehouse.gov/the_press_office/Joint-Statement-by-President-Dmitriy-Medvedev-of-the-Russian-Federation-and-President-Barack-Obama-of-the-United-States-of-America/ and Office of the Press Secretary, The White House, Hradcany Square, Prague, Czech Republic, April 5, 2009, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered/.
25. The White House, Office of the Press Secretary, "Addressing the Nuclear Threat: Fulfilling the Promise of Prague at the L'Aquila Summit," July 8, 2009, http://www.whitehouse.gov/the_press_office/Addressing-the-Nuclear-Threat-Fulfilling-the-Promise-of-Prague-at-the-LAquila-Summit/.
26. David Albright and Paul Brannan, "Surprising Admission by India's Department of Atomic Energy," September 19, 2008, http://www.isis-online.org/publications/southasia/India_DAE_19September2008.pdf.
27. Matti Tarvainen, "Unfair Trade," *IAEA Bulletin* 50, no. 2, May 2009, http://www.iaea.org/Publications/Magazines/Bulletin/Bull502/50203556163.html.
28. See Security Service, "Counter-Proliferation," Web Site, https://www.mi5.gov.uk/output/counter-proliferation.html.
29. Communication with European government and industry officials, July 1, 2008.