1

Introduction: The Problem of Black-Market Nuclear Technology Networks

Matthew Bunn and William C. Potter

In the early morning of October 4, 2003, the German-registered ship *BBC China* was detained and inspected at the Italian port of Taranto en route from Dubai to Tripoli, Libya. In the ship's hold was a cargo of centrifuge parts – products designed for enriching uranium and destined for Muammar Gaddafi's budding nuclear weapons program, provided by a global black-market nuclear technology network led by Abdul Qadeer Khan, a central figure in Pakistan's nuclear weapons program. The story of how the centrifuge parts made their way toward Libya and how they were intercepted is the stuff of fictional spy thrillers. In this instance, however, the story is all too real.

While the US government rightly hailed the demise of the A. Q. Khan network following the seizure of the *BBC China*, the problem of illicit nuclear trafficking continued. Khan's network was neither the first nor the last international network to pursue illicit trade in key technologies for nuclear weapons. The Khan network was unprecedented, however, in at least three ways. The first was the scope and scale of its operations, offering full service supply of complete centrifuge facilities to produce nuclear weapons material – along with nuclear weapon designs, instructions on casting and machining uranium metal and producing uranium hexafluoride for enrichment, and more. Second, in addition to being a demand-driven operation focused on supplying the nuclear weapons program of Pakistan and later of other states, it also became supply-driven, a network looking for customers. Finally, though the degree to which the network's operations were authorized by the Pakistani government remains disputed, most accounts conclude

that at least some of the network's activities were freelance operations, orchestrated by private entrepreneurs.[1]

Today, although the Khan network is no longer in evidence, illicit nuclear trade facilitated by others continues, and has provided support for nuclear efforts in Iran, North Korea, Pakistan, India, and, potentially, beyond. Indeed, every nuclear weapons program for decades has relied extensively on illicit imports of nuclear-related technologies.[2] While it would be unrealistic to hope that strengthened nonproliferation efforts could entirely halt black-market nuclear trade, effective steps to block illicit purchases of nuclear technology have sometimes succeeded in slowing nuclear weapons programs and increasing their costs, and they have the potential to do so in the future as well. These efforts can buy time for diplomacy to work, thereby increasing the chance that states will abandon their pursuit of nuclear weapons. Hence, success in preventing illicit transfers wherever possible is a key element of an effective global nonproliferation strategy.

The nuclear agreement reached in 2015 between Iran and the Permanent Five members of the UN Security Council plus Germany (the "P5+1") is a case in point.[3] Prior to the agreement, Iran was perhaps the leading

[1] For useful summaries of the Khan network and the larger problem of illicit nuclear trafficking, see Chapter 2 of this volume; David Albright, Andrea Stricker, and Houston Wood, *Future World of Illicit Nuclear Trade: Mitigating the Threat* (Washington, D.C.: Institute for Science and International Security, July 2013), http://isis-online.org/uploads/isis-reports/documents/Full_Report_DTRA-PASCC_29July2013-FINAL.pdf; and International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A. Q. Khan and the Rise of Proliferation Networks: A Net Assessment* (London: IISS, 2007). For additional useful accounts of the Khan network in particular, see, for example, Gordon Corera, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A. Q. Khan Network* (New York and Oxford: Oxford University Press, 2006); David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010); Adrian Levy and Catherine Scott-Clark, *Deception: Pakistan, the United States, and the Secret Trade in Nuclear Weapons* (New York: Walker, 2007); Douglas Frantz and Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets. . .and How We Could Have Stopped Him* (New York: Twelve, 2007); and Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (New York: Free Press, 2011).

[2] A partial exception is the North Korean program, where the original plutonium production reactor and reprocessing plant appear to have been largely indigenous, though North Korea may have imported some components. North Korea relied extensively on illicit imports for its centrifuge program, however – including support from the Khan network.

[3] For a description of the accord, key documents, and arguments for and against, see Gary Samore, ed., *The Iran Nuclear Deal: A Definitive Guide* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2015), http://belfercenter.ksg.harvard.edu/publication/25599/.

illicit purchaser of nuclear-related technology; much of Iran's nuclear program was based on foreign supplies.[4] The United States and other countries applied almost every supply-side tool available to slow Iran's effort, from blocking particular purchases to sabotage to broad economic sanctions. While these efforts demonstrably failed to stop Iran's program, they made it slower, more costly, and more uncertain; a strong case can be made that these supply-side efforts were among the factors that gave diplomacy and sanctions the time needed for them to work. Moreover, the agreement includes an agreed "procurement channel," in which Iran must get international approval for all purchases of nuclear and dual-use items for its nuclear programs.[5] Implicitly, this represents an acknowledgement by all parties that constraining illicit purchases of nuclear-related technology – the subject of this book – is an important element of achieving nonproliferation objectives. Effective implementation of the procurement channel will require an ongoing effort both to facilitate legitimate purchases and to ensure that illicit purchases outside the channel are not occurring.

This book attempts to offer a broad picture of the problem of illicit nuclear technology trade and what can be done to strengthen global efforts to stop it. This task is challenging, as both the illicit nuclear technology trade and the world's efforts to stop it take place largely in secret – and the constant struggle between those trying to maintain and enforce technology controls and those trying to get around them is inevitably complex. Illicit nuclear traders build networks of supplier firms, brokers, front companies, and trans-shippers that span the globe, consciously building layer after layer to cover their tracks and hide the true purpose and destination of the transfers. To be effective, the response must be as creative, adaptive, and global as the networks are. National efforts must take a "whole-of-government" approach, combining intelligence, law enforcement, export controls, interdiction, customs, and financial controls. Private companies must provide internal controls. And governments across the globe must cooperate, sharing information and working together in the effort to disrupt these networks. This book seeks to examine each of these potential opportunities for stopping this illicit trade.

[4] See Ian J. Stewart and Nick Gillard, *Iran's Illicit Procurement Activities: Past, Present, and Future* (London: Project Alpha, Center for Science and Security Studies, King's College London, July 24, 2015).

[5] For a discussion of the procurement channel, see Ian J. Stewart, "The Iranian Nuclear Procurement Channel: The Most Complex Part of the JCPOA?" *WorldECR*, 2015, www.worldecr.com/wp-content/uploads/Iranian-Nuclear-Procurement-Channel_WorldECR1.pdf.

Some definitions of terms are in order. We use the word *technology* as it is used in dictionaries, rather than as it is used in US export-control law – it refers to scientific knowledge turned to practical purposes, and to machines, equipment, and materials made with that scientific knowledge. The transfers this book concerns itself with include both shipments of physical objects – centrifuges, flow-forming machines, carbon fiber, and more – and transfers that consist only of information that can be sent at the click of a mouse, ranging from bomb designs to suggestions for overcoming a manufacturing problem. This latter category of information-only transfers is sometimes referred to as "intangible technology."

By *black-market* or *illicit* we mean that the transfers support a secret or illegal weapons-related end-use, usually through unofficial channels, in contrast to open state decisions to sell nuclear reactors or other nuclear technology to another state. In some cases, national laws may be so weak that the transfers pursued through such secret, under-the-table means are not actually illegal; when the Khan network was producing centrifuge parts for Libya's nuclear weapons program at a factory in Malaysia, for example, Malaysia had no export-control law (not having any indigenously developed nuclear technology to control). Nevertheless, we would still consider such purchases as part of the overall phenomenon of illicit trade in technology to support nuclear weapons programs.

By *network,* we mean a collection of different actors – individuals, labs, firms, and in some cases government agencies – that are cooperating to make these transfers happen. Such networks may include both conscious participants – motivated by money, support for a particular state, ideology, or other factors – and unwitting ones, who may have no idea they are facilitating nuclear weapons-related work. Nuclear entrepreneurs play an organizing role and are most likely to be found in states outside of the nuclear Nonproliferation Treaty (NPT) and the Nuclear Suppliers Group (NSG), such as North Korea (which is both an importer and an exporter of nuclear and missile technologies).

This book is about illicit procurement of the *technologies* needed to produce nuclear weapons material and nuclear weapons themselves – not about smuggling of already-produced nuclear *materials* such as plutonium and highly enriched uranium (HEU). Smuggling of nuclear material is also a critical danger that must be addressed – but to date, these two kinds of illicit smuggling appear to be separate and very different. The cases of plutonium and HEU smuggling documented in the public record largely involve small-time hustlers searching for potential buyers for their

material, with very modest levels of sophistication.[6] The market for nuclear weapons-related technologies, by contrast, is largely driven by the demands of states, and in many cases is highly sophisticated, involving large sums of money passing through complex layers of agents, brokers, and front companies designed to hide the real buyer and the real purpose of the purchases.

In short, while occasionally there may be some overlap, nuclear material smuggling and illicit nuclear and dual-use technology procurement are distinct phenomena with different actors and drivers, and require different policy responses. That being said, in some cases there may well be important synergies among responses to these threats that should be exploited, including efforts to improve implementation of international legal mechanisms such as UN Security Council Resolution 1540, to enhance border and export controls, to bolster intelligence sharing both within governments and among countries, and to foster the development of greater nonproliferation educational and training opportunities with the goal of building a more robust, global nonproliferation culture.

ILLICIT NUCLEAR TRADE IN A GLOBALIZING WORLD

Four realities are at the heart of the problem of illicit nuclear trade in the twenty-first century. First, a small number of states continue to seek nuclear weapons – and attempt to advance their weapons programs by acquiring technology abroad. Second, in a globalizing world, technology is spreading inexorably, creating essential opportunities for economic development, but also creating more firms in more countries with the potential to provide necessary technologies for nuclear weapons efforts; some key components for centrifuges that can enrich uranium to weapons-grade, for example, can now be made anywhere one can set up and operate a high-precision computer-aided manufacturing machine. Although this is not a new problem, the magnitude of the challenge has

[6] For a useful summary of nuclear material smuggling, see Lyudmila Zaitseva and Friedrich Steinhäusler, *Nuclear Trafficking Issues in the Black Sea Region, EU Non-Proliferation Consortium Non-Proliferation Papers* no. 39 (Paris: SIPRI, 2014), www.sipri.org/research/disarmament/eu-consortium/publications/non-proliferation-paper-39. For an account of the incidents in 2014 in particular, see James Martin Center for Nonproliferation Studies, *CNS Global Incidents and Trafficking Database: Tracking Publicly Reported Incidents Involving Nuclear and Other Radioactive Materials* (Washington, D.C.: Nuclear Threat Initiative, April 2015). The report and the database on which it is based are available at www.nti.org/analysis/reports/cns-global-incidents-and-trafficking-database/.

grown significantly in recent years with the proliferation of potential nuclear suppliers.[7] Third, global trade is massive and extraordinarily diverse, creating a huge number of potential exporters, traders, brokers, financiers, and trans-shippers, and making tracking illicit nuclear trade a problem of finding tiny needles in gigantic haystacks. Fourth, many of the key technologies useful for a nuclear weapons program have civilian uses as well. As just one of countless examples, uranium-enrichment centrifuges work best if they are made from material that is both very strong and very light – but strong and light materials are useful for countless other purposes.

To be sure, the dual-use problem is not a new one; from the dawn of the nuclear age, the world has been struggling to find ways to distinguish between good "atoms for peace" and bad "atoms for war." Eisenhower's famous "Atoms for Peace" initiative, and the competing US and Soviet nuclear export policies that followed, contributed to the spread of civilian nuclear technologies to many countries – technologies that in some cases were turned to military use, or could be in the future.

Many of the nuclear transfers of the 1950s and 1960s were open, legal transfers. But following entry into force of the NPT; the detonation of a "peaceful nuclear explosion" by India in 1974 and the subsequent formation of the NSG; and the discovery after the 1991 Gulf War that Iraq had built an extensive secret nuclear weapons program from technologies largely purchased in Europe and the United States, the major suppliers have placed tighter constraints on their nuclear commerce. With less technology available through open transfers, would-be proliferators increased their emphasis on getting what they wanted through illicit nuclear trade.

A POTENT EXAMPLE: THE A. Q. KHAN NETWORK

Khan's network re-shaped the terrain of nuclear proliferation. Initially designed and honed in the 1970s to provide technology for Pakistan's clandestine pursuit of nuclear weapons, Khan subsequently reoriented the network from imports to exports, and eventually presided over a partly state-directed and partly illicit business venture that spanned much of the globe. Although by no means the only nuclear black-marketer, he was by

[7] For a discussion of similar challenges in the 1980s see William C. Potter, ed., *International Nuclear Trade and Nonproliferation: The Challenge of the Emerging Suppliers* (Lexington, MA: Lexington Books, 1990).

far the most ambitious, and put into practice a business model that Dr. Mohamed ElBaradei, former Director General of the International Atomic Energy Agency (IAEA), characterized as a "nuclear Wal-Mart."[8] Since Khan was not known to have sold fully operational nuclear weapons, others have suggested that a more appropriate analogy was a "nuclear Home Depot" with the motto: "You can do it. We can help."[9]

Before its demise in 2003, the Khan network had been the leading global provider of black-market nuclear technology. It demonstrated a capability to marshal scores of individuals in more than a dozen countries in support of its commercial nuclear export activities, and while the full record of its nuclear sales has yet to be uncovered, it is known to have provided sensitive centrifuge technology to Libya, Iran, and North Korea. (The network's internal documents repeatedly refer to a fourth customer, but international investigators have not yet confirmed who that other customer was.[10]) It provided nuclear weapon designs to Libya, and possibly to others; more advanced designs than the ones found in Libya were found on the hard drives of the Tinner family, key participants in the network who lived in Switzerland.[11] The network shipped centrifuges from Pakistan, made uranium management equipment in South Africa, manufactured centrifuge components in Malaysia, and integrated packages of technology in Dubai for shipment on to its customers. The extent of the Pakistani government's involvement remains in dispute; while Pakistan asserts that Khan acted on his own, many observers believe that at least the transfers to North Korea and Iran were directed by senior officials of the Pakistani state.[12]

Surprisingly, the Khan network operated in over a dozen countries for more than twenty years before it was taken down. Moreover, nearly all of

[8] Mohamed ElBaradei, *The Age of Deception: Nuclear Diplomacy in Treacherous Times* (New York: Metropolitan Books, 2013), p. 166. ElBaradei had used the Wal-Mart analogy from shortly after the network was revealed: see, for example, Mark Landler, "U.N. Official Sees a 'Wal-Mart' in Nuclear Trafficking," *New York Times*, January 23, 2004.

[9] Congressman Gary L. Ackerman, "A. Q. Khan's Nuclear Wal-Mart: Out of Business or Under New Management?" Joint Hearing before the Subcommittee on the Middle East and South Asia and the Subcommittee on Terrorism, Nonproliferation, and Trade of the Committee on Foreign Affairs of the House of Representatives (June 27, 2007), p. 2.

[10] For a provocative argument that the fourth customer was India – undermining Khan's reputation as the patriotic savior of Pakistan – see Joshua Pollack, "The Secret Treachery of A. Q. Khan," *Playboy* (January/February 2012), http://carnegieendowment.org/files/The_Secret%20Treachery%20of%20AQ%20Khan.pdf.

[11] For a discussion, see Collins and Frantz, *Fallout*, pp. 195–210.

[12] See discussion in IISS, *Nuclear Black Markets*, pp. 67–88.

the network's participants are free men – and rich men – today, although many of them served time in jail (or under house arrest, in Khan's own case). How, one may ask, was it possible for a very entrepreneurial metallurgical engineer from Pakistan to forge a vast and diverse illicit nuclear suppliers' network and operate it for decades before the international community found out and took action? These outcomes represent an interlocking series of failures by numerous governments over many years. It was first and foremost a failure of *policy,* with many governments choosing to look the other way when evidence was ambiguous, to deal gently with allies even if they were crossing nuclear red lines, and to put higher priority on promoting exports than on controlling them. In the developing world in particular, many countries had urgent economic, health, and other developmental priorities, and understandably did not rank reducing nuclear proliferation risks near the top of their national priority lists – a problem that persists today.

But it was also a failure of *intelligence* to understand what was happening and provide sufficient actionable information to convince government to act, until very late in the game; a failure of *export controls*, with many countries having either no export controls at all or grossly inadequate export controls; and a failure of *law enforcement*, with many countries making little effort to arrest and prosecute illicit nuclear exporters, or to share information across borders necessary to make a convincing case in court. In addition, it was a failure of *customs, border controls,* and *interdiction,* as prior to the seizure of the *BBC China* virtually none of the network's transfers were stopped at borders or interdicted during shipment, and few countries had people at their borders trained to examine these kinds of goods; and a failure of *private-sector compliance programs*, as numerous companies unwittingly provided technology to the network without realizing its intended purpose (including the Malaysian factory, which reportedly believed it was providing components for the oil industry).[13] Finally, it was a failure of *nonproliferation culture*, in that few in either firms or government agencies placed top priority on stopping the spread of nuclear weapons, and those participating in the network often convinced themselves that what they were doing posed little threat to global security and might even enhance it. The network's remarkably long run can hardly be said to be a failure of *sanctions*, or of *financial controls*, as broad-scale international sanctions and financial controls intended to

[13] Raymond Bonner, "'Business as Usual' at Plant That Tenet Says Was Shut," *New York Times*, February 7, 2004.

interfere with the nuclear weapons programs of the network's customers had not yet been imposed.[14]

This book explores all of these disparate elements of the global response to black-market nuclear technology networks, seeking ways to strengthen them and prevent future failures of this kind. In each case, the key questions are: would the approaches in place today be able to stop another such network before it did similar damage? Would they be sufficient to stop future networks, as they evolve and adopt new tactics and approaches? Can we envision strengthened approaches that would help those attempting to stem the spread of nuclear weapons technology win the struggle with the black-marketers more often?

A too-exclusive focus on the countries seeking nuclear weapons technologies, rather than on the possibility that states like Pakistan or non-state networks of firms and individuals might supply them, contributed to these failures. Until the tragic events of September 11, 2001, most policymakers with responsibility for nonproliferation paid little attention to the potential for non-state actors to acquire – or supply – nuclear weapons. The text of the NPT makes no reference at all to the risks posed by non-state actors, and its prohibition on transferring nuclear weapons technology only refers to transfers to states, conducted by acknowledged nuclear weapon states. While an extensive roster of non-state players had been active in supplying material to nuclear weapons programs in Iraq, Pakistan, and elsewhere over the decades, the notion that a global network of individuals and firms not fully under the control of any state might be in a position to supply nearly all of the key ingredients of a nuclear weapons program was not on anyone's radar screen.[15] The battle within the US government over what to do about A. Q. Khan focused for many years on Pakistan's own nuclear weapons program, and how the

[14] The United States and other countries had long had unilateral sanctions in place on Iran and North Korea, driven both by nuclear issues and other concerns, but broader international sanctions on these countries were not yet in place prior to 2003 in the case of North Korea and 2006 in the case of Iran. Libya was under international sanctions for its role in the Lockerbie bombing, and these sanctions do appear on occasion to have made financing of some of its deals with the network more difficult. Saddam Hussein's Iraq was approached by the network before the imposition of sweeping sanctions, but did not take the network up on its offer before the 1991 Gulf War intervened.

[15] The question of the degree to which the network was authorized and directed by the Pakistani state, versus the degree to which it operated as an independent non-state actor or set of actors, remains hotly disputed; the Pakistani government denies having any knowledge of Khan's exports, but there is significant circumstantial evidence that some of the transfers were authorized and approved by key government figures.

United States should handle the nuclear transgressions of a difficult ally in a strategically important region – not on stopping illicit nuclear exports through a global network directed from Pakistan.

Moreover, during the Cold War, both policymakers and intelligence agencies were fixated on the threat posed by the Soviet Union. While stopping the spread of nuclear weapons was an important priority, the threat posed by Moscow, typified by the proxy war waged against the Soviet Union following its invasion of Afghanistan in 1979 – and the subsequent effort to manage the end of the Cold War – dominated US national security considerations at the highest levels of the US government.

Even after the Soviet collapse, the former Soviet states were the principal focus of concern with regard to the potential leakage of nuclear material and technology. Indeed, in the 1990s the United States put an intensive effort into attempting to block Russia's nuclear dealings with Iran, from the civilian reactor project at Bushehr to more sensitive transfers – while it is now known that at the same time, Iran was getting much of the technology the United States worried about from the Khan network. The end of the Cold War also led to significant reductions in resources devoted to human intelligence gathering and intelligence analysis, including the monitoring and assessment of new nuclear proliferation developments.[16] Today, the demands of counter-terrorism and war-fighting in Afghanistan, Iraq, Syria, and elsewhere similarly draw resources away from coping with illicit nuclear procurement networks.

Ultimately, the network headed by A. Q. Khan overreached, and intelligence and law-enforcement actions in a number of countries succeeded in shutting it down. The international community has taken numerous steps to strengthen controls in the aftermath of the revelation of the Khan network. A few of the more important steps include:

- *UN Security Council Resolution (UNSCR) 1540*, which legally obliged all states to make it a crime to provide any assistance to non-state actors seeking nuclear, biological, chemical, or missile technologies, and to put in place "appropriate effective" export controls, border controls, and trans-shipment controls. While many countries have since adopted new export-control laws, implementation remains a work in progress.[17]

[16] Corera, *Shopping for Bombs*, pp. 130–131, also notes this point.

[17] For assessments of UNSCR 1540 implementation in regions around the world, see James Martin Center for Nonproliferation Studies, *UNSCR 1540 Resource Collection* (Washington, D.C.: Nuclear Threat Initiative, June 2015), www.nti.org/analysis/reports/1540-reporting-overview/. For accounts raising questions over the effectiveness of 1540 implementation, with recommendations for improvement, see Richard T. Cupitt,