10

Countering Nuclear Black Markets by Strengthening Nonproliferation Culture

Matthew Bunn

Those seeking nuclear weapons-related technologies through black-market networks succeed only when they can find people with access to what they want who are either willing to provide it knowingly or susceptible to being duped into providing it. Building a culture in which those with access to these technologies believe strongly that nuclear proliferation is a danger to their countries and the world, and that they have a personal responsibility to slow the spread of these technologies whenever they can, would greatly reduce nuclear black-marketers' chances of success.

The focus of this chapter, then, is on building a "nonproliferation culture" – one in which the people in the companies, labs, agencies, universities, and technical communities involved in managing and controlling sensitive nuclear and dual-use technologies understand the critical importance of preventing nuclear proliferation and give that objective the attention and priority it deserves.[1] An essential complement of this nonproliferation culture is an anti-corruption culture, one in which everyone

[1] The literature on nonproliferation culture is much sparser than the literatures on the related areas of safety culture or security culture. Indeed, no internationally agreed definition of the term exists. I would define a strong nonproliferation culture as "a pervasive, shared belief among political leaders, senior managers, and operating personnel that effective measures to prevent the spread of nuclear weapons are critically important, as manifested in decisions and actions, large and small." This essentially substitutes "effective measures to prevent the spread of nuclear weapons" for "MPC&A" (material protection, control, and accounting) in a definition offered years ago of what the authors then called "safeguards culture" and would now be called "security culture." See James E. Doyle and Steven V. Mladineo, "Assessing the Development of a Modern Safeguards Culture in the NIS," *Nonproliferation Review*, vol. 5, no. 2 (Winter 1998), http://cns.miis.edu/npr/pdfs/doyle52.pdf, pp. 91–100.

understands the dangers of taking money to provide technology or look the other way.[2] Indeed, a nonproliferation culture will generally be only one element of a broader culture of integrity and responsibility in these organizations and communities.[3]

The first step is a culture of compliance, in which companies and individuals seek to scrupulously follow relevant laws and rules. Clearly, designing genuinely effective rules on limiting sensitive technology transfers and enforcing them appropriately are key elements of an overall system to combat illicit nuclear technology trafficking. Creating a real possibility of being caught and punished for breaking the rules is an important element of convincing companies and people to take these rules seriously – as is structuring the rules so that their purpose is clear and they do not unduly interfere with the normal course of business.[4] Companies are often highly motivated to avoid legal risks and risks to their corporate reputations, which can be undermined when charges against them are in the newspaper or their equipment shows up in the nuclear program of a proliferating state.

But a culture of compliance is not enough. Those seeking these technologies are clever, and they find ways to go around the rules, or to hide their violations of the rules, using front companies, routes through countries other than the final destination, false end-user certificates, and other tactics to cover their tracks.[5] Blocking such tactics requires going beyond a compliance-based culture to a culture focused on proactive efforts to achieve the goal of preventing nuclear proliferation.[6] In particular, a

[2] See Matthew Bunn, "Corruption and Nuclear Proliferation," in Robert Rotberg, ed., *Corruption, Global Security, and World Order* (Washington, D.C.: Brookings, 2009), pp. 1–48.

[3] Benjamin Heineman Jr., former Vice President and General Counsel of General Electric, offers tips on building such a high integrity culture in Benjamin Heineman Jr., *High Performance With High Integrity* (Boston, MA: Harvard Business Press, 2008). See especially pp. 25–99.

[4] See Chapter 4 by Leonard S. Spector and Chapter 5 by Mark Fitzpatrick in this volume.

[5] See Chapter 2 by David Albright and Andrea Stricker in this volume.

[6] In the related area of safety culture, the IAEA has identified three organizational stages. Stage 1 (the least effective) is "safety based on rules and regulation." Stage 2 is "safety becomes an organizational goal." Stage 3 is "safety can always be improved." Here, the objective is to move as many of the individuals and organizations handling sensitive nuclear-related technologies as possible to Stage 3 – "nonproliferation can always be improved." See International Atomic Energy Agency, *Safety Culture in Nuclear Installations: Guidance for Use in the Enhancement of Safety Culture*, IAEA-TECDOC-1329 (Vienna: IAEA, December 2002), www-pub.iaea.org/MTCD/publications/PDF/te_1329_web.PDF, pp. 17–19.

proactive approach is likely to include partnerships between companies and governments to share information on entities seeking particular technologies, suspect inquiries, best practices in reviewing export requests, and more.

To achieve such a proactive nonproliferation culture (and even to achieve compliance with export rules) is likely to require convincing people that preventing the spread of nuclear weapons technology really matters – to the security of their country, their families, and the world. Research indicates that most people will not violate rules they are convinced are important; indeed, belief in the importance of the rule is in some cases more important in reducing the number of violations than a person's estimate of the probability and consequences of being caught violating it.[7] In addition to *personal* beliefs, *organizational* culture and habits – such as the ways companies seek to ensure that potential orders are properly scrutinized and their risks assessed – are also central elements in the effort to stop nuclear technology black markets.

The question, then, is: how do we convince people in the relevant groups that rules to prevent proliferation and to counter corruption are important, and that (a) they should not violate them, and (b) they should be actively on the look-out for suspicious activities and opportunities to strengthen controls? If large proportions of them *are* convinced of these things, it will be much more difficult for those seeking illicit transfers of technology to recruit willing suppliers.

THE DANGERS OF WEAK NONPROLIFERATION AND ANTI-CORRUPTION CULTURES

Learning from past failures and successes is a key theme of this book. An examination of the history of the A. Q. Khan network and the black-market networks initiated to supply the nuclear programs of Iraq and Iran makes clear that weak nonproliferation and anti-corruption cultures in the 1970s and 1980s were a major problem that helped these networks succeed – in Europe, the United States, and elsewhere.

Interviews with participants in the A. Q. Khan network make clear that many of them convinced themselves of a Waltzian view that nuclear proliferation did not pose a major security threat, as more states with

[7] James Reason, *Managing the Risks of Organizational Accidents* (Aldershot, UK: Ashgate, 1997), pp. 145–146.

nuclear weapons would mean less chance of major war.[8] Peter Griffin, for example, says that he told investigators: "I believe that if everybody's got a big stick that's more security for the world than only a couple of people having big sticks."[9] Henk Slebos, another Khan network participant, said "I am proud that I have prevented a number of wars" by helping Pakistan get the bomb.[10] Moreover, some participants in black-market nuclear technology networks offer the easy excuse that "if I don't sell, someone else will."

For people that got involved long ago, these attitudes may not be surprising. In the 1970s, when Khan was first establishing his network, nonproliferation norms were weak. The nuclear Nonproliferation Treaty (NPT) had just come into force and many countries were not yet parties; export-control laws and procedures were nascent or non-existent; many countries were more focused on promoting nuclear exports than on controlling sensitive ones; and India had just conducted a nuclear test, making it easy for participants to convince themselves that it was "only fair" that Pakistan should have the bomb as well.[11]

Moreover, at that time, anti-corruption norms were also weak, and accepting an under-the-table payment for working around a rule controlling a particular technology was much more common than it is in advanced developed democracies today. The illicit Iraqi purchase of 100 tons of maraging steel in 1988 – estimated by Mahdi Obeidi, the purchaser, as enough for 10,000 centrifuges, capable of producing material for 15 nuclear bombs per year – was so clearly understood as corrupt by all participants that some of the key discussions took place in a strip club in Paris.[12]

Today, the belief that preventing the proliferation of nuclear weapons is important to world security is much more widespread and anti-corruption

[8] For the "proliferation optimist" view of Kenneth Waltz, see Scott D. Sagan and Kenneth N. Waltz, *The Spread of Nuclear Weapons: An Enduring Debate*, 3rd edn. (New York: Norton, 2012).

[9] Quoted in Steve Coll, "The Atomic Emporium: Abdul Qadeer Khan and Iran's Race to Build the Bomb," *The New Yorker*, August 7, 2006, www.newyorker.com/archive/2006/08/07/060807fa_fact_coll?currentPage=all.

[10] Quoted in Frank Slijper, *Project Butter Factory: Henk Slebos and the A. Q. Khan Nuclear Network* (Amsterdam: Transnational Institute, September 2007).

[11] For descriptions of the culture and the weakness of proliferation controls at the time, see for example, 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), pp. 1–48.

[12] Mahdi Obeidi and Kurt Pitzer, *The Bomb in My Garden: The Secrets of Saddam's Nuclear Mastermind* (Hoboken, NJ: Wiley & Sons, 2004), p. 101.

measures are much more extensive, particularly in developed countries. But the constant drumbeat of cases of people selling technology that might be used in a nuclear weapons program to countries under sanctions or under suspicion of pursuing nuclear weapons, coupled with the lack of proactive efforts to find and stop dangerous transactions at many companies, make clear that some of the attitudes and habits of the past are still in place.

There is both good news and bad news from efforts to build a strong nonproliferation culture among all the companies, institutes, agencies, and technical institutes involved in managing and controlling sensitive nuclear technology. The good news, as described below, is that a number of key companies have drastically changed their approach and shifted from past active or passive participation in proliferation to current proactive efforts to work with governments, other companies, and nongovernment organizations to stop proliferation.

The bad news is two-fold. First, many relevant companies or institutes have *not* gone through a comparable cultural transformation. Second, experience suggests that changing deeply ingrained organizational cultures is very difficult to do.[13] In general, organizational cultures change only slowly – in response to either a crisis that appears to threaten the survival or well-being of the organization, or transformative leaders who make it their mission to change the organization's culture, or both.

NONPROLIFERATION CULTURE AT COMPANIES

As discussed by Robert Shaw in Chapter 7 chapter of this book, the private sector plays a critical role in the effort to control sensitive technologies. Companies – both private and state-owned – are the places where building a strong nonproliferation culture matters most, as they are the center of the world's export markets and the predominant place where those seeking to acquire nuclear-related technologies go to try to get them.

[13] For a useful discussion of the requirements for making substantial changes in the way an organization performs its functions, and the many ways such efforts fail, see John P. Kotter, *Leading Change*, 1st edn. (Boston, MA: Harvard Business School Press, 1996). A classic text on organization culture is Edgar H. Schein, *Organizational Culture and Leadership*, 3rd edn. (San Francisco, CA: Jossey-Bass, 2004). A substantial portion of academic writers on organizational culture believe even these authors are too optimistic about the ability of leaders to really change an organization's culture in the absence of an event (or series of events) that creates substantial survival anxiety in the organization.

There are essentially three ways in which a firm might find itself participating in nuclear technology black markets:

- the firm's management itself may decide to conspire to provide sensitive technology to proliferators;
- an individual or small group at a firm may decide to conspire in that way, without the knowledge of management; or
- the firm might be duped into providing technology without realizing it was going to a nuclear weapons program.

As noted above, to avoid these outcomes, particularly the third, firms must go beyond simply avoiding violations of export-control rules to proactively seeking to stop illicit nuclear transactions – identifying weaknesses in existing controls and discussing them with the government, communicating with the government about suspicious inquiries, and exchanging best practices with others in their industry.

This is a tall order. Millions of companies, large and small, exist around the world. Thousands of companies handle some material or technology that would be helpful for a nuclear weapons program. Fortunately, it appears that a number of key "chokepoint" technologies on the path to nuclear weapons are supplied by only a handful of firms around the world (though this may change as globalization and technological change proceed).

The relevant firms fall along several spectra, each of which affects their roles in this problem:

- **Size.** On one end of this spectrum, immense global firms such as General Electric, Toshiba, or Siemens are likely to have significant knowledge for controlling nuclear-related exports; specialized staff devoted to that purpose; relationships with the governments in the countries in which they operate; and the ability to forego a potentially suspect contract because it is only one tiny part of their broader business. (Even they, however, can sometimes be fooled by a sophisticated procurement effort shrouded in layers of front companies and trans-shipments hiding the real purpose and end-user.) By contrast, a very small firm may have only limited understanding of the potential weapons applications of a technology it supplies or of the specifics of the export-control rules surrounding that technology, few staff or resources to assess such risks, limited ability to get advice from relevant government officials, and may find giving up a $1 million contract much more difficult to do.

- **Sensitivity.** For some companies, the reason they are not intimately familiar with export controls is that the technologies they work with are not especially sensitive. The SCOPE factory in Malaysia, for example, which manufactured centrifuge components for the A. Q. Khan network, had never handled nuclear technologies, and thought they were making parts for the oil industry. Though they were making centrifuge components, these were not among the most difficult-to-manufacture components; items such as bearings and maraging steel bellows were to be manufactured elsewhere. For other companies, their technology is highly sensitive and more likely to be a target of export bans or restraints.
- **Nonproliferation commitment**. Some companies have already decided to make preventing proliferation a priority, taking an approach based on the goal of nonproliferation, which goes well beyond simply following the rules. Others are committed to following the rules, but not to anything more. Still others may not devote much energy to understanding and following the rules. A small minority is consciously willing to flout the rules to sell their technology. An obvious goal for governments and non-government organizations is to influence as many of the most sensitive companies as possible to shift toward the truly committed, goal-based category.
- **Environment**. Where a firm is operating is also important. In developed industrial states, strong laws are in place that technology firms largely follow, and networks of consultants and lawyers are available to help a company understand export controls and identify those trying to circumvent them. A company operating in western China or Siberia, by contrast, may have few resources available to help it work through what transactions it should and should not engage in, and may be competing against other firms willing to sell the same technology to anyone.

Traditionally, a great deal of the work in export controls has focused on improving the performance of already reasonably high-performing companies in the United States, Europe, and a few other developed countries. But companies in other categories may be higher priorities for efforts to strengthen nonproliferation cultures. In particular, companies should be high priorities for government or non-government organization outreach where: (a) the sensitivity of their technology is high (especially if it is a key "chokepoint" technology on, for example, the path to centrifuges or the path to weaponization); (b) their commitment to nonproliferation and the degree to which they operate in a supportive environment are both

comparatively low, suggesting that without action they might be at risk of being exploited by black-market nuclear technology purchasers; and (c) they previously have been targets of states known to engage in illicit procurement activities.[14]

Two key questions need to be answered. First, how can companies that wish to establish a strong nonproliferation culture achieve that objective? Second, how can companies best be convinced that they *should* establish a strong nonproliferation culture? Consider two case studies of success in changing corporate culture on these topics – Leybold AG (now part of the Oerlikon Group) and Toshiba. Both are multinationals headquartered in advanced, developed countries; Leybold before its absorption into Oerlikon was a much smaller and more specialized firm, while Toshiba is a global conglomerate. In both cases, sweeping changes were provoked by company-threatening export mistakes.

In the 1970s and 1980s, Leybold, a supplier of vacuum technologies and precision machining equipment, was a key supplier for Iraq's nuclear program and for the A. Q. Khan network. After the 1991 Gulf War, inspectors in Iraq discovered Leybold equipment that was being used in centrifuge manufacture. The company faced a US criminal investigation, embarrassment that affected its brand, and the potential for substantial business losses.[15] The company's board brought in a new management team who made it their mission to change the company's approach to nonproliferation. The new management team issued a clear policy statement – the Leybold Charter – making clear that "Leybold attaches

[14] See, for example, the work that the UK government-sponsored Project Alpha, at King's College, has done in reaching out to Chinese firms in sensitive technology areas.

[15] Leybold's dismaying record of proliferation in the 1970s and 1980s (including as the original institutional base for key A. Q. Khan network participants such as Gotthard Lerch and Daniel Geiges) is discussed in David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010). After discussing numerous incidents of poor behavior by Leybold in the past, Albright devotes an entire chapter to discussing the company's turnaround and its new approach to controlling technology as a model for other companies to follow. See pp. 227–243. For an earlier account focused only on Leybold's supplies to Iraq, see David Albright, "The Lessons of Leybold" (Washington, D.C.: Institute for Science and International Security, June 1993), http://isis-online.org/isis-reports/detail/building-a-corporate-nonproliferation-ethic/. For accounts from Leybold itself, see Ralf Wirtz, remarks at the panel on "Finding Innovative Ways to Detect and Thwart Illicit Nuclear Trade," Carnegie International Nonproliferation Conference, June 26, 2007, http://carnegieendowment.org/files/detect_thwart.pdf; and Andreas Widl (CEO, Oerlikon Leybold Vacuum), address to the Carnegie International Nonproliferation Conference, March 28, 2011, http://carnegieendowment.org/files/Atoms_for_Peace.pdf.

clear-cut and unambiguous priority to the goal of nonproliferation of nuclear weapons and their delivery systems over commercial interests," and directing that "all Leybold employees will actively assist in the achievement of this corporate goal." Further, the Charter established the policy that whenever there was "any continuing concern" about the end-use of an item to be exported, the company "will not conclude the transaction."[16]

Beyond the clear policy statement, the company established new export-control review processes; new training on export controls throughout the firm; and new relationships with the German and US governments. When doubts about a particular request for a piece of equipment arose, the company would now consult with German and US officials. It regularly received information on suspected front companies to watch out for and provided information on suspicious inquiries it was receiving, a relationship that has proved fruitful for both the firm and the governments involved. Leybold estimates that it has turned down some $50–$60 million in business since putting the new policy in place.[17]

The broad outlines of Toshiba's story are similar, though the companies and the specifics are quite different. In the 1980s, Toshiba Marine, a subsidiary of the larger firm, falsified export documents in order to ship high-precision machine tools to the Soviet Union, for use in making quieter submarine propellers.[18] Toshiba Marine's management was directly involved. The resulting scandal and criminal investigation dramatically jeopardized Toshiba's global position; in Washington, Toshiba products were being smashed on the steps of Capitol Hill, and one senator proposed legislation that would ban all of Toshiba from doing any business at all in the US market for five years.[19]

As with Leybold, this shock to the system caused the top leadership at Toshiba to conclude that it needed a radically different approach to export controls. The head of Toshiba Marine resigned, Toshiba as a whole adopted new top-level corporate policies on export controls, and Toshiba established focused processes to review potential exports for both compliance with the law and appropriateness. Training in the new

[16] The full text of the original 1992 Leybold Charter, and the more recent one issued by Oerlikon, are available in Institute for Science and International Security, "The Leybold Charter: Putting Non-Proliferation Above Commercial Interests" (Washington, D.C.: ISIS, 2010); www.isis-online.org/peddlingperil/ch11/leybold_directives.

[17] Albright, *Peddling Peril*, p. 229.

[18] See, for example, David Sanger, Clyde Haberman, and Steve Lohr, "A Bizarre Deal Diverts Vital Tools to Russians," *New York Times*, June 12, 1987.

[19] Author's interview with Robert Shaw, March 2013.

approaches permeated the company. When Robert Shaw, author of Chapter 7 on the role of the private sector, joined the company years later, on the first day of training he was told to expect to make many mistakes during his time at Toshiba, and to learn from them – but that in the area of export control, not a single mistake could be permitted.[20]

In both of these cases, a dramatic shock was required to motivate the company's leadership to change course. But once those decisions were made, the companies succeeded in changing their corporate culture surrounding export controls, becoming far more responsible global players – and enhancing their brands in the process.[21] Clearly, however, it is important to find ways to motivate companies to take such actions *before* they become embroiled in such company-risking catastrophes – perhaps by using such examples as cautionary tales of what can happen to a company that lacks a strong nonproliferation culture.

What then, should the leadership of a company seeking to build a strong nonproliferation culture within their organization do?[22]

- **Policy.** Companies should adopt clearly articulated policies, put forward from the highest levels of the organization, identifying preventing proliferation as a key priority of the organization and the responsibility of everyone. The Leybold Charter is an example. In today's world of global outsourcing, the policy and all the other steps the firm takes should apply not only to what goes on within the firm itself, but to its entire global supply chain as well.[23]
- **Communication and training.** Companies need to communicate the importance of preventing proliferation throughout the organization, including through the actual actions of leaders of the organization and through training programs. Actions speak louder than words, and

[20] Ibid.

[21] The fact that both the Oerlikon (formerly Leybold) company official in charge of proliferation prevention and Oerlikon's CEO have been invited to speak as examples of what other companies should do at the international nonproliferation conferences sponsored by the Carnegie Endowment for International Peace is a striking example of the enhancement to the company's brand that resulted from the new policy.

[22] The suggestions below are similar in many ways to the suggestions for creating a high-integrity corporate culture in Heineman, *High Performance With High Integrity,* pp. 25–99.

[23] Ian Stewart, the founder of Project Alpha, has made this point particularly strongly. See, for example, Ian J. Stewart, *Antiproliferation: Tackling Proliferation by Engaging the Private Sector* (Cambridge, MA: Project on Managing the Atom, Harvard University, November 2012), http://belfercenter.ksg.harvard.edu/files/Antiproliferation-Layout-final.pdf.

could include spending time on nonproliferation issues, complimenting and rewarding individuals who succeed in identifying and stopping deals that could contribute to proliferation, dealing firmly with corporate officials who fail to build strong nonproliferation approaches within their organizations over a sustained period of time, and proactively reaching out to government agencies to strengthen the organization's nonproliferation performance. Training should include programs to help employees understand: (a) the importance of nonproliferation to the company, to the national security of the country where the staff are living, and to the security of the world; (b) technological pathways to proliferation and how their company's technology might be related to them; (c) entities seeking nuclear weapons-related technology and the tactics they use, including factors that might make a particular purchase request suspect; and (d) corporate policies and procedures and legal rules governing controls on sensitive technologies and their export. The training should be designed so that by the end of it, employees know both *how* they are expected to control sensitive technology transfers and *why*.

- **Incentives.** Changing a company's culture requires changing employees' incentives. If employees are still rewarded only for meeting sales targets, they will be tempted to turn a blind eye to some red flags in order to make a major sale. Companies need to put in place systems that reward employees for excellence in nonproliferation performance – for example, bonuses for identifying and stopping important suspect transfers, or for identifying ways to strengthen the firm's nonproliferation approaches.[24]
- **Focused teams.** Companies cannot expect to achieve excellence in nonproliferation performance unless they create teams of highly qualified experts to take charge of the issue, and give them the authority and resources needed to do their jobs. Much of the success at Leybold, for example, can be attributed to Ralf Wirtz, the export-control expert who has led their nonproliferation effort for years – and to the top corporate managers who supported his efforts.[25]

[24] For a discussion of the related topic of incentives for excellence in nuclear security, see Matthew Bunn, "Incentives for Nuclear Security," *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., July 10–14 2005* (Northbrook, IL: INMM, 2005).

[25] See, for example, discussion in Albright, *Peddling Peril*, pp. 227–243.

- **Reporting systems.** Giving employees a voice is critical to building a culture in which all employees take responsibility for contributing to preventing proliferation. Companies should establish ombudsman programs that give employees the opportunity to report mistakes and make suggestions without fear of reprisal, and anonymous reporting systems that encourage employees to report any wrongdoing or questionable behavior. And it is essential that employees perceive that the company takes such concerns seriously and addresses them appropriately.
- **Assessment programs.** Developing metrics for how well a company is performing in an area like nonproliferation is extraordinarily difficult. Issues such as how many times the government has raised questions about the company's exports, or how the company has done in government reviews of its program should certainly be tracked and assessed, but may not tell the whole story. In particular, if the number of incidents of potentially suspect transfers going ahead is going down, is that because fewer such transfers are being made, or because employees are no longer rating such transfers as suspect, or because those seeking to proceed with such transfers have gotten better at evading controls and cloaking the transfers in respectability? If reports of suspect transfers are increasing, is that because the problem is getting worse or the reporting system is getting better? One area that companies *should* try to track is the nonproliferation attitudes of their employees – the beliefs that drive culture and behavior. Companies should carry out regular surveys, asking questions about how important employees think it is to prevent nuclear proliferation, how much priority they see this goal as having within the company, what they would do if there were only modest doubts about a potentially very lucrative export, and more.[26] These surveys should then be used as tools to identify areas for improvement, driving a culture of continual improvement in nonproliferation performance.

Of course, companies will differ in their capability to implement such measures, depending on where they fall on the spectra described above. Governments and NGOs should put in place programs to help companies that want to build a strong nonproliferation culture but need additional resources or expertise to do so.

[26] For guidance on using such employee surveys to assess the somewhat related area of safety culture, see IAEA, *Safety Culture in Nuclear Installations*.

Beyond the issue of capacity, however, there is the issue of commitment. Many companies have not yet decided to make nonproliferation a priority. Governments and NGOs should identify the companies handling the most sensitive technologies – and those that may be able to provide such technologies in the near future – and work to convince them that it is in their corporate interests to make nonproliferation a priority. Both frank discussions of the dangers nuclear proliferation poses to their countries and the world, and cautionary tales of the corporate risks of export-control missteps (such as those that befell Leybold and Toshiba) may help persuade companies to take such steps. Putting together coalitions of firms committed to nonproliferation – as Kings College's Project Alpha is seeking to do, with its "Partners in Antiproliferation" program – can also help convince corporate managers of the value of adopting stringent nonproliferation policies as a corporate policy. Such coalitions can work to produce industry benchmarks and best practices, so that firms have a common understanding of what they should be doing, and have fewer concerns about being undercut in the market – at least by other firms within the coalition.

Beyond simply keeping a close eye on a firm's technology transfers, two elements of a reformed nonproliferation culture in private companies are particularly important. The first is building a real partnership between private firms handling the most sensitive technologies and governments. This partnership should be a two-way street. Firms should serve as lookouts for governments, reporting on suspicious inquiries and the entities behind them; governments should work with firms to make sure they know about entities and types of purchases to be on the lookout for, and should absolve them of any liability they might incur by providing suspicious inquiry information to governments.

The second is building concern for nonproliferation into firms' entire global supply chains. While small firms in emerging markets may be less committed to nonproliferation and in a less supportive environment, they will put in place effective nonproliferation approaches if global companies that are some of their biggest customers insist on it. Moreover, by integrating their monitoring of suspicious inquiries over many markets, global firms can observe which entities are making similar requests in different countries.[27]

[27] For a Leybold example, see Albright, *Peddling Peril*, p. 235.

NONPROLIFERATION CULTURE AT GOVERNMENT LABORATORIES

Some government laboratories also handle highly sensitive technologies that must be effectively controlled. This problem, while real, is generally less severe than the problem of private companies, for several reasons:

- There are many fewer government laboratories than private companies handling potentially sensitive technologies.
- While government laboratories are sometimes in need of revenue, they do not have the profit focus and export-driven approach that private companies have.
- Governments have much greater control over their laboratories than they have over private companies (or even state-owned enterprises, in some cases).
- The culture in government laboratories working with sensitive technologies is already generally focused on national security as a key mission of the organization.

Nonetheless, there have been a variety of cases of illicit exports from government laboratories over the years. The most spectacular, of course, were the exports from what were then called the Khan Research Laboratories in Pakistan as part of the A. Q. Khan network. But there have been others, with leakages of technology from laboratories in the United States, Russia, and elsewhere.[28]

The steps the leadership of a government laboratory can take to achieve a strong nonproliferation culture in the organization are similar in many ways to those described above in the case of private firms. In

[28] Examples range from the accidental sale for scrap of the equipment for a plutonium reprocessing plant from a US government laboratory to the participation of a former Soviet implosion systems designer in implosion work in Iran – ostensibly designed for creation of nanodiamonds. Another incident – with more involvement of top laboratory leadership – involved the sale of ballistic missile guidance systems taken from Russian strategic ballistic missiles to Iraq, at a time when Iraq was under sanctions and such sales were illegal. The guidance systems were tested and certified at the laboratory before being exported. See Vladimir Orlov and William C. Potter, "The Mystery of the Sunken Gyros," *Bulletin of the Atomic Scientists*, vol. 54, no. 6 (November/December 1998), pp. 34–39. For a survey of Russian scientists and engineers that appeared to reveal a strikingly weak nonproliferation culture in the 1990s, see Deborah Yarsike Ball and Theodore P. Gerber, "Russian Scientists and Rogue States: Does Western Assistance Reduce the Proliferation Threat?" *International Security*, vol. 29, no. 4 (Spring 2005), pp. 50–77.

some countries, laboratories may have a more command-and-control system than private companies, making it easier for the organization's management to reward and punish employees for their nonproliferation performance; in others (including in the United States), the employees of government laboratories may actually have more job protection than employees of private firms do, making such rewards and punishments more problematic.

Here, too, governments and NGOs should identify those laboratories likely to pose the highest risks – those handling the most sensitive technologies and which do not score well on commitment to nonproliferation or the degree to which they operate in an environment supportive of nonproliferation performance – and seek to work with them to strengthen their nonproliferation cultures.

NONPROLIFERATION CULTURE IN GOVERNMENT AGENCIES

A strong nonproliferation culture is also critical in the government agencies charged with controlling trade in sensitive technologies. An export ministry more concerned with promoting exports than controlling them, an export-control reviewer susceptible to being bribed, a customs officer who does not bother to check whether the boxes contain what the manifest says they contain – any of these can seriously weaken the effectiveness of a country's controls on exports or trans-shipments of sensitive technologies.

As with companies, different governments (and different agencies within particular governments) vary widely in their commitment to nonproliferation. For those seeking to build up a strong nonproliferation culture, many of the tools for doing so are similar to those described above for private firms.[29]

Governments and NGOs seeking to get other governments to strengthen their agencies' focus on nonproliferation should take several steps. First, they should analyze the on-the-ground implementation of controls over the most sensitive technologies, seeking to identify the gaps and problems that pose the highest risks of technology leakage. Second,

[29] Most of the recent literature on changing organizational culture has been produced in business schools and focuses on private firms. The literature on steps to change the culture of a government agency is much smaller. As one contrary example, see Robert Behn, *Performance Leadership: 11 Better Practices That Can Ratchet Up Performance* (Washington, D.C.: IBM Center for the Business of Government, 2006); www.businessofgovernment.org/sites/default/files/PerformanceLeadership.pdf.

they can work on two parallel tracks to address these high-priority challenges: (a) efforts to convince these agencies of the importance of achieving high nonproliferation performance (and of the strong nonproliferation culture needed to achieve that objective), and (b) programs to help these agencies institute training programs, incentive systems, reporting structures, and similar measures to strengthen their nonproliferation culture and performance. In other words, they should focus on both capacity-building and commitment-building at the same time. These two kinds of efforts are both essential, and relate closely to each other; capacity-building programs often end up identifying and building up experts who push internally for more progress, while commitment-building efforts can help increase agencies' willingness to put their own resources behind sustaining increased capacity.

NONPROLIFERATION CULTURE AT UNIVERSITIES

Nonproliferation culture is important at universities for two reasons. First, universities must avoid inadvertently spreading sensitive technologies through their teaching and research activities. Second, universities should sensitize students being trained in fields where they may end up handling sensitive nuclear-related technologies to the proliferation issues and professional responsibilities they may face – one element of building up a broader nonproliferation culture in key technical communities, discussed below.

But universities present problems that are very different from those posed by private companies or government laboratories. The essence of universities is generating and imparting knowledge. Academic freedom – including open discussion among all students and faculty – is a core value. In the United States, many of the leading research universities (including Harvard) prohibit any secret research from being done on campus, and some will reject funding for research projects if the government insists on excluding foreign students from participating in them.[30] Many believe that the absence of officially secret information means they do not need to focus very much on the potential sensitivities of the information they do have. Each faculty member is an independent actor, making the creation of a unified culture extremely difficult. In short, universities generally do not put top priority on controlling the spread of information and technology.

[30] I have personally been told not to apply for research grants that carried this stipulation at Harvard University.

Nevertheless, the leaders of many universities understand that controls on particularly sensitive technologies are necessary, and understand the risks to their universities that export-control missteps could pose. Large universities often have portions of their legal offices devoted to export controls, and some training available for faculty and staff who seek it out. Moreover, many universities have extensive experience with the related issues involved in protecting intellectual property that may have commercial value.

The most difficult issues export staff and faculty at universities have to cope with arise from intangible "deemed exports" – when imparting information to a foreign student, or involving a foreign student in research that develops new knowledge about a particular technology, is considered an "export" of technology to the nation the student is from. (One Texas researcher was sentenced to four years in prison for violations of the Arms Export Control Act after involving a Chinese doctoral student in an Air Force-sponsored research project restricted to US citizens.[31]) It is comparatively rare for a university to officially approve an actual export of a sensitive piece of technology to a foreign country.

Despite the efforts now in place, universities, including large research universities with established export-control programs, remain potential sources of technology leakage. At many institutions, especially smaller ones, a culture of awareness of such nonproliferation issues is absent across much of the university.

What can be done to improve nonproliferation culture at universities? Getting key faculty and staff to understand the rules and how they apply to their classes and research is the first step. The United Kingdom has developed special guidance for universities.[32] Among other steps, the guidance suggests that universities issue clear policy statements on the importance of export-control compliance; provide training to all research faculty and staff; include export-control issues in reviews of the ethics of

[31] See Project Alpha, "John Reece Roth and Export Control," (London: King's College, June 13, 2013) one of the case studies available from Project Alpha, at http://projectalpha.eu/?s=John+Reece+Roth. Roth insists that his work should be considered research in the public domain, not subject to the Arms Export Control Act. It does appear, however, that he willfully did not follow the requirements the Air Force contracting officials attempted to impose.

[32] See Association of University Legal Practitioners and Project Alpha, "Higher Education Guide and Toolkit on Export Controls and the ATAS Student Vetting Scheme" (London: King's College, April 2, 2015); http://projectalpha.eu/academia.

research proposals; and establish a clear point of contact for export-control questions.

But universities, like private firms, should seek to go beyond compliance to proactive efforts to prevent proliferation. The issue should be discussed at key faculty meetings in the most relevant departments. Individual faculty or staff members should be designated as nonproliferation leaders for their units of the university (for example, a department or research center), and should develop and implement plans for strengthening nonproliferation culture in their unit.[33] These culture coordinators from across the university should meet regularly to discuss ways to move the agenda forward. And like private companies, universities should use surveys of employee attitudes to assess the progress of their culture-change activities and identify the highest priority areas that require remedial attention.

At the same time, the university has a responsibility for inculcating a nonproliferation culture among students working in potentially sensitive technological areas. Today, this responsibility is often not being met. At many universities, it is possible to get a Ph.D. in nuclear engineering without having had a single lecture on nonproliferation or nuclear security.[34] This should change. All students graduating with technical knowledge that could contribute to a nuclear weapons program should have instruction in the importance of nonproliferation and their personal responsibility to prevent it. There is a long way to go to achieve that objective.

NONPROLIFERATION CULTURE IN KEY TECHNICAL COMMUNITIES

Beyond these formal institutions, there is the question of the culture in broader technical communities whose members might have the expertise to contribute to a nuclear weapons program. Governments and NGOs should seek to identify particular technical communities that should be high priorities, and reach out to them. In the case of centrifuges, for

[33] In the related area of security culture, as a result of US–Russian nuclear security cooperation, Russia has established such culture coordinators at many of the key nuclear facilities controlled by Rosatom, the Russian state nuclear corporation.

[34] Until recently, for example, at MIT, one of the leading US nuclear engineering departments, there were two courses in which the topic of nonproliferation was mentioned. One devoted one lecture in a semester to the topic, the other two. Both were electives, so it was possible (even likely) to get a doctorate in nuclear engineering without having received a single lecture on nonproliferation. Now MIT has two full-semester courses devoted to nonproliferation issues in the nuclear engineering department (both electives).

example, one would want to focus on people in the specialized world of vacuum engineering; people who know about making and using maraging steel; and people who know about making and using good-quality carbon fiber (among other technical areas).

What tools could help strengthen nonproliferation culture in these key technical communities? The most powerful – beyond the efforts at various organizations described above – are likely to be training, codes of professional conduct, and discussions in professional societies.

Training. As noted above, universities should seek to ensure that all students who receive training in technical fields that could contribute significantly to nuclear weapons programs – including but certainly not limited to nuclear engineering – are aware of the security risks posed by nuclear proliferation, and of their responsibility to help prevent it. Companies and laboratories, as they train employees for the first time in sensitive technology areas, should also provide training on these nonproliferation issues.

Codes of professional conduct. The idea that being a member of a profession carries with it certain professional responsibilities – including ethical responsibilities – is now quite widespread, going far beyond the medical profession's Hippocratic Oath. Often codes of professional conduct are developed by professional societies, to be signed by all their members. As just two of countless examples, the Association of Computing Machinery (ACM) and the Institute for Electronic and Electrical Engineering (IEEE) each have codes for their members, which commit them to broad principles of conduct. For example, ACM members are committed to 24 items, beginning with commitments to "contribute to society and human well-being" and to "avoid harm to others."[35]

Governments and NGOs should work with relevant professional societies to develop appropriate elements related to nonproliferation for their professional codes of conduct, committing participants not to contribute to illicit nuclear weapons programs and to proactively seek to prevent the spread of nuclear weapons and sensitive technologies.[36]

[35] See Association for Computing Machinery, "Code of Ethics," www.acm.org/about/code-of-ethics.

[36] One effort in Japan sought to convince nuclear experts to sign a "Peace Pledge": "I, undersigned below, pledge with honor and dignity: To the best of my knowledge, I will not participate in the research, development, production, acquisition and utilization of nuclear weapons as well as of other weapons of mass destruction." For present purposes, it would be necessary to go further and include provisions committing participants not to

Discussions in professional societies. The role of professional societies might go beyond codes of professional conduct to hosting discussions and publishing papers that could help sensitize their members to nonproliferation issues. It could be extremely useful, for example, to publish accounts of past cases and lessons learned in widely read professional society newsletters or journals, with a call for discussion of what should be done to prevent such events in the future.

CONCLUSIONS

Strong nonproliferation cultures in companies, laboratories, agencies, universities, and technical communities involved in handling sensitive nuclear-related technologies could do a great deal to reduce the probability that people seeking such technologies illicitly would succeed in getting them. Nonproliferation culture in many organizations and communities is already far stronger than it was in the 1970s. But there is a great deal yet to do to build awareness and commitment to preventing the spread of nuclear weapons and the technologies needed to make them.

These issues of nonproliferation culture affect and are affected by many of the other efforts to stop black-market nuclear technology trafficking discussed in this volume. If countries establish clear and effective export-control rules, for example, and enforce them – so that serious violators suffer major fines and jail time – this will certainly have an effect on the culture surrounding these technologies, in private companies and elsewhere. If better international intelligence and law-enforcement cooperation created a higher probability that participants in such networks would be caught and punished, the incentives to participate would be reduced and it would be easier to build sufficient counter-incentives to convince people never to take part in such networks. And if stronger nonproliferation cultures could be built in the organizations discussed in this chapter, this could strengthen essentially every other element of the global effort to stem illicit trafficking in these technologies. It could lead to more reporting from companies of suspect inquiries; closer scrutiny of proposed exports; more willingness within law-enforcement and intelligence organizations to devote the needed resources and to cooperate with each other; more focus on the issue from international organizations; and other knock-on effects.

participate in any transfer of sensitive technology that could contribute to a nuclear weapons program, and to proactively seek to prevent proliferation.

The media also play an important role. The more that leading Western media outlets, especially those such as the BBC that boast substantial global audiences, cover the proliferation threat, including reports on the punishments inflicted on those failing to comply with export-control or sanctions policies, the more they will contribute to building a common feeling that taking part in schemes that contribute to the spread of nuclear weapons is immoral and should not be tolerated. This can significantly reinforce the appreciation of nonproliferation norms at the business, institutional, and personal levels.

Ultimately, much of the effort to control the spread of nuclear weapons is based on human behavior and choices, which in turn are strongly influenced by beliefs about what actions are right and wrong, how important different priorities are, and what steps are worth taking – in short, by culture.

Box 10.1: The Danger Posed by Former Employees

Most nonproliferation programs focus on people at known companies and laboratories. Government-sponsored outreach programs are designed to sensitize known companies in key industries to relevant export-control rules and how to recognize potentially suspect purchase requests. US nonproliferation assistance programs designed to re-employ former weapons scientists in the former Soviet Union focused only on the experts who were still at their laboratories or institutes, ignoring those who had retired or moved to other employment.

But the experience of past illicit nuclear technology trafficking suggests that some of the gravest proliferation risks come from people who have left the company or laboratory where they first gained access to sensitive technologies. Gotthard Lerch, Friedrich Tinner, Peter Griffin, Henk Slebos, Daniel Geiges, and Gerhard Wisser, to name a few – all key players in the A. Q. Khan network – were men who left the kinds of companies that might be included in a nonproliferation partnership with a government, and set up their own businesses. No government outreach program to legitimate businesses would have reached those new firms.

Similarly, Vyacheslav Danilenko, the former Soviet implosion systems designer who participated in implosion projects in Iran – ostensibly to produce nanodiamonds – had left the Snezhinsk weapons design laboratory years before, and had his own small firm in Ukraine. Nonproliferation policymakers must keep the risks posed by such individuals "outside the system" in mind, and develop policies to reduce those risks. In particular, governments should keep track of who has had access to particular types of sensitive information

and technology – both within the government and its laboratories and at private companies – and what those people are doing today.

Programs to strengthen nonproliferation culture such as those discussed in this chapter can only reduce these "former employee" risks indirectly – in two ways. First, if legitimate companies build stronger nonproliferation cultures, they will be less likely to supply sensitive technology to such outside-the-system operators (who often have trouble arranging to manufacture such items themselves). Second, if a strong nonproliferation culture grows up in key technical communities, people with similar skills will be less likely to choose to leave legitimate firms or government laboratories and follow an illicit path in the future.