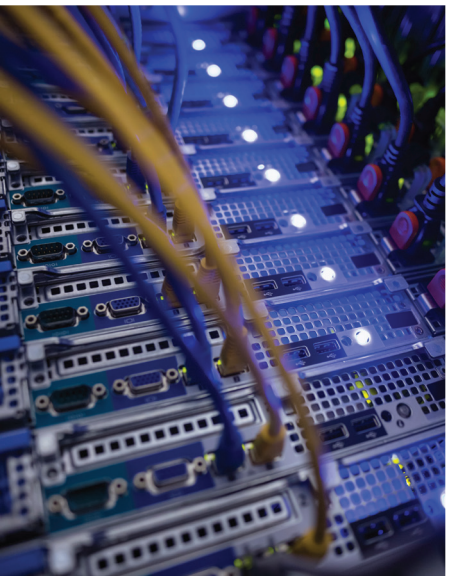
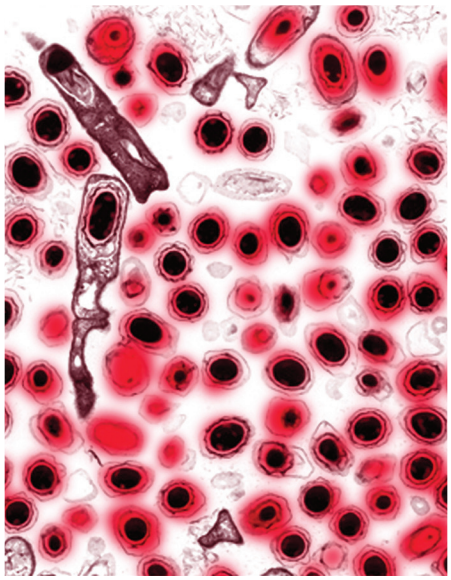
Governance of Dual-Use Technologies:
Theory and Practice


Elisa D. Harris, Editor

AMERICAN ACADEMY OF ARTS & SCIENCES

Governance of Dual-Use Technologies: Theory and Practice

Elisa D. Harris, Editor

ISBN:0-87724-110-4

This publication is available online at https://www.amacad.org/gnf.

Suggested citation: Elisa D. Harris, ed., *Governance of Dual-Use Technologies: Theory and Practice* (Cambridge, Mass.: American Academy of Arts & Sciences, 2016).

Cover images (from left): Interior rack of mounted servers © 2014 by iStock.com/Wavebreakmedia; *Bacillus anthracis* bacterial spores, Centers for Disease Control and Prevention (CDC) Public Health Image Library (PHIL), added color by Scott Camazine; nuclear power plant cooling towers © 2013 by iStock.com/vencavolrab.

This paper is part of the American Academy's Global Nuclear Future Initiative, which is supported in part by grants from Carnegie Corporation of New York, The William and Flora Hewlett Foundation, The John D. and Catherine T. MacArthur Foundation, The Alfred P. Sloan Foundation, The Flora Family Foundation, and The Kavli Foundation. The statements made and views expressed in this publication are those held by the authors and are not necessarily those of the Officers and Members of the American Academy of Arts & Sciences or the foundations supporting the Global Nuclear Future Initiative.

Please direct inquiries to:
American Academy of Arts and Sciences
136 Irving Street
Cambridge, MA 02138-1996
Telephone: 617-576-5000
Fax: 617-576-5050
Email: aaas@amacad.org
Web: www.amacad.org

Contents

This volume is dedicated to the memory of
John D. Steinbruner—teacher, mentor, colleague, friend,
and inspiration to generations of students and analysts of
global security challenges and responses.

Acknowledgments

The authors are grateful to the diverse group of experts who participated in the American Academy of Arts and Sciences meeting on "Dual-Use Technology: Current and Future Governance Prospects," held at the Chicago Council on Global Affairs in March 2015. We are especially grateful to Steve Fetter, David Fidler, the late Roger Hurwitz, R. Scott Kemp, Gregory Koblentz, and Jens Kuhn for their thoughtful comments on the draft papers presented at the meeting, and to Jo Husbands, Susan Koch, and Angela McKay for enriching our meals with their insightful presentations. We would also like to thank Rebecca Lordan and Kristopher Pittard for their assistance in transcribing the meeting discussions.

Special thanks are also owed to those who took the time to review and comment on subsequent drafts of the chapters published in this volume. In particular, James Acton thanks Togzhan Kassenova for her comments on the draft and Lauryn Williams for her research assistance. Herbert Lin thanks Stephanie Forrest, Trey Herr, David Relman, and Adam Segal. Elisa D. Harris thanks Seth Carus, Richard Ebright, Thomas Holohan, Jo Husbands, Gregory Koblentz, and Milton Leitenberg for their detailed comments and suggestions, and Kathryn Harris, David Koplow, and Kathryn Nixdorff for their insights on particular issues.

We also are extremely grateful to the leaders of the Academy's Global Nuclear Future Initiative—Robert Rosner, Steven Miller, and Scott Sagan—for their assistance in developing this project, their input during the March 2015 dual-use technology meeting, and their subsequent comments on this volume. Finally, we want to extend our deepest gratitude to Francesca Giovannini and Kathryn Moffat at the Academy for the extraordinary support and assistance they provided throughout this project.

Preface

Robert Rosner

Modern concerns about dual-use technologies emerged in concert with fears about the proliferation of nuclear weapons–related technologies in the early days of the Cold War. These concerns focused on obvious targets, such as specialty steels, high-precision computer-aided manufacturing tools and facilities, and high-performance software and hardware; that is, materials and tools that are readily adapted to nuclear weapons–related design and manufacturing. More recently, focus has shifted to nonnuclear technological contexts—including, most prominently, biological and information technology—in which ongoing research and development has dramatically advanced human social and economic well-being, though at the cost of generating potential for these technologies to be harnessed for nefarious purposes.

Of course, the dual nature of technological advances—capable of elevating humanity and unleashing destruction upon it—long predates the total war and scientific breakthroughs of the twentieth century. For example, the chemical advancements underlying the use of fireworks in imperial China were adapted by the tenth century AD to produce "fire arrows" for use in battle.[1] What has changed since is not the balance of dual-use technologies, but the ability of modern weaponry to kill on drastically greater scales, affecting vast portions of the earth's surface—a dynamic captured in J. Robert Oppenheimer's sobering allusion to the two-thousand-year-old *Bhagavad-Gita*: "I am become Death, the destroyer of worlds," when describing the Trinity nuclear explosion.[2] We are faced today with weaponry that is appropriately referred to as weapons of mass destruction.

Given these stakes, how can we create effective international and national governance structures that provide a legal framework for regulating the flow of powerful dual-use technologies, as well as provide for enforcement mechanisms ensuring compliance with it? Technological innovation consistently follows a course of "trickle-down" effects: what is high precision today is run-of-the-mill tomorrow; capabilities once considered rare and extraordinary, and thus condu-

1. One of the earliest recorded uses of such rockets in warfare was the defense of the Chinese city of Tzu T'ung in AD 994.

2. Oppenheimer quoted from Swami Prabhavananda and Christopher Isherwood, trans., *Bhagavad-Gita: The Song of God* (Madras, India: Sri Ramakrishna Math, 1945), ch. xi, v. 32. The line is elsewhere given as "I am become Death, the shatterer of worlds."

cive to control, evolve to become the ordinary, slipping outside any possibility of enforceable regulation. The most obvious example is the evolution of computer technologies: the Herculean effort of the analog computers of the Manhattan Project is today totally eclipsed by the computing power of any budget-model laptop loaded with freely available modeling software. Similarly, computer-aided design and manufacturing has evolved over the past two decades such that the tools for high-precision manufacturing have become commodity products: a complete CAD/CAM (computer-aided design and computer-aided manufacturing) workshop, including extremely high-precision numerically controlled machining tools, can be assembled today at costs easily within the reach of well-funded terrorist groups.

In response to these challenges, the American Academy's Global Nuclear Future Initiative, which I direct alongside Steven Miller and senior advisor Scott Sagan, decided to take a comprehensive look at the range of current efforts to constrain dual-use technologies—that is, efforts to create dual-use governance structures—with a particular focus on their effectiveness in controlling the spread of technologies that can have both beneficial and harmful consequences. The modern touchstone of such efforts has, as stated above, been the control of technologies that enable the construction of nuclear weapons; thus, a significant component of our study is an examination of the similarities and differences between the strategies used in the nuclear realm and those proposed for biological and information technology.

We began with a series of small workshops in 2012 that sought to introduce and explore the critical issues surrounding dual-use technologies; these workshops led to a larger meeting held at Stanford University in January 2013, from which we drew the conclusion that to reach a useful understanding of the dual-use issue, we needed to significantly narrow our focus. Ultimately, we organized our strategic approach around governance: What have we learned about the potential for dual-use technology control from the decades-long efforts to restrict the spread of technology related to nuclear and biological weapons and, more recently, cyber weapons?

To this end, we were fortunate to enlist Elisa D. Harris to lead a follow-on effort focused on these questions (and to address the issue of biological technology), and to convince James Acton and Herbert Lin to offer their views on the governance issues in the nuclear and information technology domains, respectively. The authors prepared detailed background papers that were discussed extensively at a meeting held in Chicago in March 2015. This volume contains revised versions of the papers presented by James Acton, Herbert Lin, and Elisa Harris at that meeting, together with introductory and concluding chapters by Elisa Harris.

Three painful reminders of how challenging the issue of dual-use governance is emerged from our discussions. First was the realization—obvious in retrospect—of how distinct the governance challenges are in the three technological domains we have chosen to study. For example, while there is general

agreement internationally on the need to restrict access to the technologies enabling the development of nuclear weapons (with, of course, some considerable disagreements about implementation), no such consensus exists in the biological and information technology domains. Indeed, with biotechnology research, there is considerable opposition from the biological science community to any attempts to limit access to or dissemination of research findings, including information that could lead to great harm. And in the information technology arena, the Golden Rule—do unto others as you would have done to you—goes largely ignored: national adversaries (and, in some cases, allies) routinely infiltrate each other's networks to gain intelligence and network information (including the identification of vulnerabilities allowing future exploitation), to conduct economic espionage, or to cause damage directly.

Second, models of effective governance presume the capability to identify and punish violators of its terms. While there is some degree of attribution possible in the nuclear realm—including, for example, limited means of fingerprinting radioactive materials to trace them back to their origins—attribution is far more complex in the bio domain and may be practically impossible in the case of information technology. Finally, the issue of enforcement bedevils even the best understood of the dual-use realms. Consider the recent challenges in negotiating the terms of an agreement to limit Iran's nuclear program, and the pronounced failure of internationally supported sanctions to curtail the nuclear ambitions of North Korea.

Nevertheless, it is a remarkable fact that—even in light of these governance limitations—the number of major violations of the Nuclear Non-Proliferation Treaty (NPT) remains very small. This, perhaps, offers hope that with further research, analysis, and vision like that presented in this volume, we will not end up with a nuclear, biotechnology, and cyber weapons free-for-all in the twenty-first century.

This Occasional Paper is part of the American Academy's Global Nuclear Future Initiative, which is supported by generous grants from Carnegie Corporation of New York, The William and Flora Hewlett Foundation, The John D. and Catherine T. MacArthur Foundation, The Alfred P. Sloan Foundation, The Flora Family Foundation, and The Kavli Foundation.

Introduction

Elisa D. Harris

Since shortly after the first and, thus far, only use of atomic weapons, in 1945, scientists, policy analysts, and government officials have sought to identify measures to inhibit the further acquisition and use of the enormous destructive potential of nuclear technology. In the late 1960s, a similar group of stakeholders initiated efforts to prevent the biological sciences from being used to develop weapons whose destructive effects against humans, animals, and plants could, in some circumstances, rival those of nuclear weapons. Today, questions are being raised about how to manage the potential threat posed by information technology, whose growth and spread some believe may position cyber weapons alongside nuclear and biological weapons in the elite club of technologies capable of unleashing massive harm.

These technologies differ in their legal status and characteristics. But they also have one critically important similarity: each is what has come to be called *dual-use*. Over the years, this concept has been defined in various ways. The European Commission (EC), for example, defines dual-use goods as "items, including software and technology, which can be used for both civil and military purposes."[1] The U.S. government's *Code of Federal Regulations* takes a similar approach, describing "items that can be used both in military and other strategic uses . . . and commercial applications."[2] These definitions focus on the inherent characteristics of the technology and are consistent with how the term *dual-use* is used in discussions of nuclear technology.

Other definitions, however, focus more on what one analyst has called externalities, such as the context in which the technology is used, or the users themselves.[3] This is reflected in the 2004 National Academy of Sciences (NAS) report, *Biotechnology Research in an Age of Terrorism*, which describes the dual-use dilemma in biology as "when the same technologies can be used legitimately

1. "Council Regulation (EC) No 428/2009 of May 5, 2009," *Official Journal of the European Union* (May 29, 2009): L134/3, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF.

2. "Dual Use Exports," *Code of Federal Regulations*, Title 15, § 730.3 (2000), https://www.law.cornell.edu/cfr/text/15/730.3.

3. Brian Rappert and Caitriona McLeish, *A Web of Prevention: Biological Weapons, the Life Sciences and the Governance of Research* (London: Earthscan, 2007), 196–199.

for human betterment and misused for bioterrorism."[4] An externally driven approach is also evident in the work of analysts at the Center for International and Security Studies at Maryland, whose proposal for oversight of dual-use biotechnology research extends to research that is intended for beneficial purposes but can also cause harm, either inadvertently or as a result of deliberate malfeasance.[5] This definition is even broader than that used by the NAS in that it includes not just deliberate misuse of dual-use technology but accidents and other unintended outcomes.

Whatever definition one uses, military measures such as deterrence, defense, and reprisal are clearly of limited value in preventing dual-use technologies that are widely available around the globe, such as biological and information technology, from being used for hostile purposes. In both of these areas, the difficulties associated with identifying the source of an attack, or what is called attribution, render deterrence and reprisal much less effective. The technology also favors the offense over defense; that is, a biological or cyberattack is generally easier to carry out than to defend against. The situation is different in the nuclear area, where the technology is not as broadly disseminated and where measures such as deterrence, defense, and reprisal have for almost seventy years played a major role in preventing the use of nuclear weapons. They also have helped convince at least some countries that their security does not require them to use their civilian nuclear technology to develop a nuclear weapons capability.

Today, the range of actors who could cause harm with these dual-use technologies includes not just state-level actors like national governments, but also nonstate actors such as terrorists or criminals. In the case of biological and information technology, private and commercial entities and even individuals must also be considered. Moreover, distinctions between these actors often are blurred, as in the case of biodefense research, which might be funded by a government agency but conducted at a private facility. The types of harm that can result from the misuse of these dual-use technologies are similarly wide ranging and include everything from mischief to loss of life to damage to commercial, macroeconomic, or national security interests.

Because of the complexities of the threat, a wide range of different governance measures have been developed to mitigate the risks from dual-use technologies. Like the term *dual-use*, the concept of governance has been defined in a variety of ways. Noah Webster's 1828 dictionary, for example, describes it in terms of "government; exercise of authority; direction; control."[6] Political scientist Mark Bevir has more recently defined *governance* more broadly, as

4. National Research Council, *Biotechnology Research in an Age of Terrorism* (Washington, D.C.: National Academies Press, 2004), 15.

5. John D. Steinbruner, Elisa D. Harris, Nancy Gallagher, and Stacy M. Okutani, *Controlling Dangerous Pathogens: A Prototype Protective Oversight System* (College Park: Center for International and Security Studies at Maryland, 2007).

6. Noah Webster, *American Dictionary of the English Language* (1828), http://webstersdictionary1828.com/Dictionary/governance.

"all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language."[7] This definition describes some of the potential sources, targets, and forms of governance, but its descriptions are more illustrative than comprehensive.

Bevir's definition omits two elements that are important to the governance of dual-use technology: the levels at which governance is undertaken and the objectives it seeks to achieve. Each level of society is in fact potentially relevant to governance—the international, national, local, and individual. As for the objectives of governance of dual-use technologies, these can be thought of in terms of general concepts like nonproliferation, security, and safety, or in terms of more-specific goals, including:

- preventing dual-use technologies from being developed and used for hostile purposes;
- controlling access to the materials, equipment, and information or knowledge associated with dual-use technologies; and
- promoting the safe and secure handling and use of materials, equipment, or information associated with dual-use technologies.

As the following chapters show, just as no single definition of *dual-use* or *governance* is relevant to all three of these technologies, no single governance approach can mitigate the risks posed by different dual-use technologies. Nevertheless, the concept of dual-use technology is a useful organizing principle for examining governance efforts across different technology areas. This examination is especially important given the pace of technological developments and the continuing diffusion of dual-use materials, equipment, and information around the globe. These trends are playing out differently in each of the technology areas examined in this volume, but their potential consequences are the same: an increase in the risk that dual-use nuclear, biological, or information technology will cause harm, potentially on a massive scale.

Responding to this challenge requires a deeper understanding of how governance efforts in each of these areas have evolved: What types of governance measures have been adopted? What objectives have they sought to achieve? How have the technical characteristics of the technology affected governance prospects? Who are the key stakeholders and what has been their role? What have been the primary obstacles to effective governance? What gaps exist in the current governance regime? Are further governance measures feasible? These are among the questions that the following chapters on nuclear, biological, and information technology seek to address.

The discussion in each of these chapters will lay the foundation for an analysis of governance arrangements across the three dual-use technology areas: What are the most important differences among the technologies, and to what

7. Mark Bevir, *Governance: A Very Short Introduction* (Oxford: Oxford University Press, 2013), 1.

extent do they affect governance prospects? What are the most important similarities in the governance measures being used in the different technology areas? What factors account for the limitations in the various governance measures that have been adopted to date? Are further governance measures feasible in any of these technology areas? Finally, what lessons can be learned about dual-use technology governance from the experience of these particular dual-use technologies? These questions will be the focus of the volume's concluding chapter.

Chapter 1

On the Regulation of Dual-Use Nuclear Technology

James M. Acton

INTRODUCTION

When General Electric acquired the rights to Silex laser enrichment technology in 2006, few people, even within the nuclear industry, took much notice. After decades of research, laser-based technologies appeared to be yet another in a long list of enrichment processes that were not commercially viable. In 1999, the United States Enrichment Corporation (USEC), a private company originally created by the government to lead domestic enrichment efforts, had abandoned the U.S. indigenous laser enrichment program after twenty-seven years and more than $2 billion had been spent.[1] At the time, USEC had a partnership agreement with Silex Systems, the Australian company that had developed its eponymous laser-based process. But in 2003, USEC decided the technology was too expensive to commercialize and turned its attention to the gas centrifuge, which then, as now, dominated the global market for enrichment. Silex looked dead in the water.

General Electric, which merged its nuclear operations with Hitachi in 2007 to form GE Hitachi Nuclear Energy, had more success with Silex, however, and proceeded with plans to commercialize it, albeit behind schedule.[2] In 2009, it

1. The history of U.S. efforts, as well as the differences between various laser enrichment processes, are summarized in Jack Boureston and Charles D. Ferguson, "Laser Enrichment: Separation Anxiety," *Bulletin of the Atomic Scientists* 61 (2) (March–April 2005): 16, http://www.cfr.org/content/thinktank/Ferguson_BAS_separation.pdf.

2. General Electric originally intended to submit the license application by December 2007. Luis A. Reyes, memorandum to the Commissioners, "Status of the Silex Project Proposed by General Electric Nuclear," SECY-07-0031, Nuclear Regulatory Commission, February 9, 2007, 2, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2007/secy2007-0031/2007-0031scy.pdf.

submitted a license application to the U.S. Nuclear Regulatory Commission (NRC) for a commercial-scale facility. GE Hitachi indicated that a decision to build the facility would not be made until the results of further testing were known.[3] But the prospect that the United States might license a first-of-its-kind laser enrichment facility marked an important potential juncture for both the nuclear industry and the nuclear nonproliferation regime.

The benefit of the technology was clear. If laser enrichment were cheaper than the centrifuge, GE Hitachi's investment in a risky technology would reap considerable profits. (Consumer benefits, if any, would be much more modest, because the price of enrichment is set by the most expensive supplier on the market and because enrichment typically accounts for no more than 5 percent of the total cost of electricity.)[4]

The costs and risks of laser enrichment—including proliferation—were potentially significant but extremely hard to evaluate.[5] One key issue was how the commercialization of laser enrichment by a U.S. company would affect its spread globally. Would the demonstration that laser enrichment was a profitable enterprise inspire other states to attempt to develop it for themselves? Could GE Hitachi keep classified details of the Silex process secret for decades, potentially against repeated attempts by foreign governments to acquire them? Even if it could, would other states or companies nonetheless succeed in developing this or another form of laser enrichment technology from scratch? Conversely, if the United States refused to license the plant, would Silex Systems attempt to transfer the technology to another state? If so, could the United States prevent the company from doing so?

A second issue was the consequences of the spread of laser enrichment technology. Did any technical barriers prevent Silex technology from being used to produce the highly enriched uranium (HEU) needed for a nuclear weapon?[6] GE Hitachi had boasted that a Silex facility would be smaller and use less energy than a centrifuge facility—but did that not also imply that a clandestine laser enrichment facility would be more difficult to detect? How effective would International Atomic Energy Agency (IAEA) safeguards be if applied to a laser enrichment facility?

3. GE Hitachi Nuclear Energy, "Global Laser Enrichment Submits License Application to Build First Commercial Uranium Enrichment Plant Using Laser Technology," press release, June 30, 2009, http://www.businesswire.com/news/home/20090630006219/en/Global-Laser-Enrichment-Submits-License-Application-Build.

4. Geoffrey Rothwell, "Market Power in Uranium Enrichment," *Science & Global Security* 17 (2009): 136–138, http://www.princeton.edu/sgs/publications/sgs/archive/17-2-3-Rothwell.pdf.

5. For a short but trenchant discussion of the issues see R. Scott Kemp, "SILEX and Proliferation," *Bulletin of the Atomic Scientists*, July 30, 2012, http://thebulletin.org/silex-and-proliferation.

6. Although a definitive conclusion is impossible to reach without access to classified information, theoretical considerations suggest that molecular laser isotope separation processes, which include Silex, are considerably more suitable for HEU product than atomic vapor laser isotope separation. Allan S. Krass, Peter Boskma, Boelie Elzen, and Wim A. Smit, *Uranium Enrichment and Nuclear Weapon Proliferation* (London: Taylor and Francis, 1983), 165–166, 170–171, http://books.sipri.org/files/books/SIPRI83Krass/SIPRI83Krass.pdf.

To this author at least, the outcome of a cost-benefit analysis of laser enrichment technology was not obvious. *None* of the important questions was straightforward. Answers to some of them required classified information, which was secret for good reason. Others hinged on difficult-to-make political judgments. A net assessment of Silex technology would have been a difficult and controversial exercise. The U.S. government, however, did not even try. The executive branch ignored the issue. The NRC argued that its nonproliferation role extended no further than overseeing GE Hitachi's procedures for handling classified information; everything else was, in the NRC's opinion, the executive branch's responsibility.[7] While a few lawmakers did take an interest in the subject, Congress as a whole did not.

In September 2012, the NRC licensed the facility. In the three years the process had taken, nonproliferation considerations had essentially been ignored. Remarkably, the only entity with detailed knowledge of the Silex process that had attempted to analyze those considerations was GE Hitachi itself—and its assessment, which was not made public, was reportedly just seven pages long, three of which were the biographies of the authors.[8]

More than three years later, GE Hitachi has still not decided whether to build the facility. Nonetheless, its license application highlights issues—substantive and procedural—that reoccur in domestic decisions about the development and deployment of nuclear technologies. The story also illustrates the role of the global nuclear nonproliferation regime—IAEA safeguards most notably—in trying to ensure that the nuclear technology that does spread is used only for peaceful purposes.

Scoping the Dual-Use Problem

Which technologies and materials are dual-use; that is, useful for both civilian and military ends? Separated plutonium and HEU are the two dual-use nuclear materials of greatest proliferation significance. Both have a few nonmilitary applications, most notably in reactor fuel, but can also be used as the fuel for a nuclear weapon. HEU is usually defined as uranium "enriched" to contain more than 20 percent of the isotope uranium-235 (natural uranium, by contrast, consists of 99.3 percent uranium-238 and only 0.7 percent uranium-235). Although uranium enriched to any level above 20 percent is capable of sustaining the uncontrolled chain reaction used to generate energy in a nuclear weapon, practical warhead-making considerations dictate the use of HEU with an enrichment level of at least 80 percent. Whether the plutonium contained in the spent fuel discharged from modern power reactors is suitable for weap-

7. Timothy C. Johnson, memorandum to Brian W. Smith, "May 10, 2012, Meeting Summary: General Electric-Hitachi Public Meeting on Safety Evaluation Report and Final Environmental Impact Statement," Nuclear Regulatory Commission, May 22, 2012, 5, http://pbadupws.nrc.gov/docs/ML1213/ML12138A098.pdf. See also Kemp, "SILEX and Proliferation."

8. Elaine M. Grossman, "Closely Held Report Discounts Proliferation Risk of Lasers for Making Nuclear Fuel," Global Security Newswire, May 24, 2012, http://www.nti.org/gsn/article/closely-held-report-discounts-proliferation-risk-lasers-making-nuclear-fuel/.

onization has been the subject of considerable debate (its isotopic composition is quite different from plutonium produced specifically for weapons).[9] Nonetheless, the IAEA treats almost all plutonium as weapon-usable.[10] It regards twenty-five kilograms of uranium-235 in the form of HEU or eight kilograms of plutonium as the "the approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded."[11] This definition has been criticized by experts who argue that even a relatively unsophisticated proliferator could design its first nuclear weapon with less material (a nation with experience in weapon design can certainly manufacture a warhead with less material, but the agency's detection efforts are not focused on such states).[12]

Enrichment (concentrating uranium in the isotope uranium-235) and reprocessing (separating plutonium from spent fuel) are the most sensitive nuclear technologies, since they can produce weapon-grade materials. But enrichment is also vital to nuclear energy, since most power reactors in operation today use fuel made from low enriched uranium (LEU, which has a uranium-235 content between that of natural uranium and HEU). By contrast, most states, with some notable exceptions—including France, Japan, Russia, and the United Kingdom—have chosen not to reprocess the spent fuel produced by their nuclear power programs.

Nuclear technologies other than enrichment and reprocessing (such as nuclear reactors) and nuclear materials other than plutonium and HEU (such as spent fuel and LEU) are less proliferation sensitive but are still dual-use because they can be involved in the production of weapon-grade materials.

Some materials and technologies that do not involve uranium or plutonium are also of proliferation concern. First and most important, nuclear facilities involve numerous nonnuclear components. Those that also have nonnuclear applications are often described, particularly in the world of export controls, as "dual-use." This usage of the term is subtly but confusingly different from describing plutonium as dual-use because it has both civilian and military applications. In any case, certain types of pressure transducers, which can be used to monitor the operation of a gas-centrifuge enrichment plant and serve a similar function in other industrial processes, are but one example of equipment that has both nuclear and nonnuclear uses. Similarly, the nonnuclear technology

9. For example, J. Carson Mark, "Explosive Properties of Reactor-Grade Plutonium," *Science & Global Security* 4 (1) (1993): 111–128, http://scienceandglobalsecurity.org/archive/sgs04mark.pdf; and Bruno Pellaud, "Proliferation Aspects of Plutonium Recycling," *Comptes Rendus Physique* 3 (7–8) (2002): 1067–1079.

10. The only exception is plutonium consisting of more than 80 percent plutonium-238.

11. IAEA, *IAEA Safeguards Glossary: 2001 Edition*, International Nuclear Verification Series 3 (Vienna: IAEA, 2002), 23, http://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/PDF/NVS3_prn.pdf.

12. Thomas B. Cochran and Christopher E. Paine, *The Amount of Plutonium and Highly-Enriched Uranium Needed for Pure Fission Nuclear Weapons* (Washington, D.C.: Natural Resources Defense Council, 1995).

used in nuclear warhead manufacture can also be dual-use, even if its nonnuclear applications are often military. Technology for "shaping" high explosives, for example, is used in producing both antitank munitions and the explosives that are used to detonate a nuclear weapon.

Second, computer codes and other theoretical tools can have both military and civilian nuclear applications. For example, computer codes used to model the core of nuclear reactors or the behavior of plasma or the transport of radiation under certain conditions may be adaptable for use in nuclear-weapon studies. Finally, fissile materials other than HEU or plutonium could also be used to manufacture a nuclear weapon. The most important such material is uranium-233. The United States has tested nuclear warheads incorporating this material and has a stockpile of it (which it is currently trying to dispose of).[13] Furthermore, the development of thorium breeder reactors, which India is pursuing, could lead to the large-scale production and separation of uranium-233. Other alternative fissile materials (most notably, neptunium-237) are of lesser concern since they have not been (and currently appear unlikely to be) separated on a significant scale—although this could change.

Efforts to manage these technologies and materials are generally divided into nuclear nonproliferation and nuclear security. These terms have no universally accepted definitions.[14] For the purposes of this chapter, *nonproliferation* is used to refer to the goal of preventing states that do not have nuclear weapons from acquiring them. The aim of nuclear security efforts is to prevent the unauthorized possession of nuclear material or access to nuclear facilities under civilian control. In practice, most states' nuclear security efforts are directed primarily against nonstate actors, although state-based threats to nuclear security cannot be ignored.

These definitions reflect the focus of this chapter—the oversight of dual-use technology. In other contexts, *nuclear security* is often defined in a broader sense to include, for example, preventing unauthorized access to nuclear weapons or material under military control. This is clearly an important goal, but it falls outside the scope of this chapter, since nuclear weapons and military fissile materials are not dual-use. Likewise, preventing unauthorized access to radioactive but nonnuclear materials (which is sometimes considered to be part of nuclear security) and preventing the unintended release of radiation from nuclear facilities (which is always considered within nuclear safety) are also important. However, both goals have significant differences—in terms of the potential approaches to risk mitigation, the challenges to their implementation, and the consequences of

13. Robert Alvarez, "Managing the Uranium-233 Stockpile of the United States," *Science & Global Security* 21 (1) (2013): 53–69, http://scienceandglobalsecurity.org/archive/sgs21alvarez.pdf.

14. For a discussion of how the definition of *nuclear security* is evolving, see Nuclear Security Governance Experts Group (NSGEG), *Responsibility beyond Rules: Leadership for a Secure Nuclear Future* (NSGEG, March 2013), 6–7, http://www.nsgeg.org/NSGEG_Responsibilty_Beyond_Rules_2013.pdf.

failure—from nuclear security, as defined above. Finally, many analysts and officials, particularly from the Global South, would argue that nuclear nonproliferation should include not just preventing the spread of nuclear weapons to new states (sometimes termed "horizontal proliferation") but also preventing those states that have nuclear weapons from qualitatively or quantitatively enhancing their arsenals ("vertical proliferation"). While a narrower definition has been adopted here for the sake of conceptual clarity, the extent to which enhancing nonproliferation efforts is made more difficult by a perceived lack of progress on disarmament is discussed below.

A CONCEPTUAL OVERVIEW OF REGULATION

At the beginning of 1942, the practical applications of the newly emerging field of nuclear science still lay in the future. However, the promise of one potential application—the Bomb—had just sparked the creation of what came to be called the Manhattan Project. Within two years, the United States would become the first nation to operate a nuclear reactor, to separate plutonium from spent fuel, and to enrich uranium. Only after the war were these technologies used for more peaceful ends. From a historical perspective, therefore, nuclear technology is not a civilian enterprise that happens to have military applications, but a military technology that also has peaceful uses.

To manage the risks associated with this technology, an extraordinarily complex system has emerged: legally binding and politically binding agreements; norms; patterns of interstate cooperation; intergovernmental, nongovernmental, and domestic institutions; and national laws and practices (along with a bewildering number of acronyms). In fact, two largely separate systems have emerged: one for nonproliferation and one for nuclear security.

In the broadest of terms, the nuclear nonproliferation regime consists of three key interrelated elements:

- National decisions about whether to develop or use a particular dual-use nuclear technology.
- National laws and international agreements about whether to permit the sale of dual-use nuclear technologies and materials and, if so, under what conditions.
- International oversight mechanisms to detect and deter attempts by states to acquire nuclear weapons using these technologies and materials.

The importance of these three elements stems from the characteristics of nuclear technology and the way it has been developed.

First, national governments have been—and remain—absolutely central to the development and operation of nuclear technology. States or state-owned companies operate many, if not most, of the nuclear facilities around the world

today. Even nuclear facilities that are operated by genuinely private entities, such as some utilities in the United States, are dependent on governments. At the very least, a nuclear facility must be licensed. While the primary function of licensing is ensuring safety, the process requires a government to have made a policy decision in favor of permitting (or at least not prohibiting) the activity in question. In most cases, however, governments do much more than merely tolerate a nuclear activity. For example, the development of American light water reactor technology (which has now been incorporated into Chinese, French, Japanese, and South Korean designs) was originally sponsored by the U.S. government for use in submarine propulsion. Meanwhile, efforts to encourage the construction of nuclear power reactors invariably require government intervention, even in states without centrally planned economies. The United Kingdom, for example, has guaranteed the price of electricity generated by new nuclear reactors, whereas the United States offers loan guarantees to subsidize their construction. Silex laser enrichment technology is another case in point. Although efforts to develop it appear to have started as a purely private enterprise, commercialization has involved a U.S.-Australian treaty permitting its transfer to the United States (which was seeking, as a matter of national policy, to acquire an alternative enrichment process to gaseous diffusion), followed by financial assistance from USEC.

There are, of course, some exceptions—particularly where less sensitive activities are concerned. Some suppliers of nonnuclear components for nuclear facilities are private companies that did not benefit from government assistance. But, overall, governments occupy a central place in the process of developing and deploying nuclear technologies.

As a result of the centrality of governments, their internal decision-making processes about acquiring dual-use nuclear technologies assume tremendous importance in influencing the prospects for managing such technologies. To be sure, if a government wants nuclear technology because it is embarking on a campaign to develop nuclear weapons, internal oversight mechanisms are unlikely to prevent it from proliferating. However, internal processes should be important in helping a state ascertain how its domestic programs might affect the behavior of others and hence influence global proliferation dynamics—although, in practice, as the licensing process for GE Hitachi's laser enrichment plant exemplifies, states generally fail to capitalize on this opportunity because they do not have such procedures in place.

A second important characteristic of nuclear technology is that its spread—so far—has been relatively limited. About 110 states are estimated to have some capability in the manufacture of the dual-use, nonnuclear components used in nuclear facilities.[15] Seventy-one states and Taiwan conduct what the IAEA terms "significant nuclear activities," which means that they possess more than

15. Mark Hibbs, *The Future of the Nuclear Suppliers Group* (Washington, D.C.: Carnegie Endowment for International Peace, 2011), 23, http://carnegieendowment.org/files/future_nsg.pdf.

a certain amount of nuclear material.[16] Meanwhile, just nine states operate both enrichment plants and reprocessing plants, five operate enrichment plants (but do not reprocess), and one operates a reprocessing plant (but does not enrich).[17] Moreover, the group of intellectual property holders is more limited still. Enrichment plants in the United States and France both use centrifuges designed by the Anglo-Dutch-German consortium Urenco, supplied under a "black box" arrangement that prevents the operator from learning classified design details. France supplied Japan with an industrial-scale reprocessing plant and is considering whether to supply one to China. The international market for nuclear power reactors currently consists of vendors from just seven countries (Canada, China, France, Japan, Russia, South Korea, and the United States).[18]

Nuclear technology may well diffuse much more widely in the future. Nonetheless, the small number of technology holders is an important feature of today's world. In consequence, nuclear trade between the "haves" and "have-nots" has an important influence on proliferation dynamics. Therefore, decisions by states about whether, and under what conditions, to trade in nuclear technologies and materials, as well as various international export control arrangements, constitute a second important element in the nuclear nonproliferation regime.

Of course, trade is not the only way a state can acquire nuclear technology. Information can be stolen. Three of the states that operate enrichment plants today—Iran, Pakistan, and North Korea—use centrifuges based on technology illicitly acquired from Urenco, and Brazil and India may do so too.[19] States can also develop technology indigenously—and an increasing number are likely to have the capability to do so in the future.[20] The regulation of trade nonetheless continues to play an important role in nonproliferation efforts because the financial and technical barriers to entering the nuclear technology field are still relatively high. Developing the technology to enrich uranium on a meaningful scale, whether accomplished entirely indigenously or by using illicitly acquired information and components, is likely to cost at least a few hundred million

16. As of June 2013. Australian Safeguards and Non-Proliferation Office, *Annual Report 2012–13* (Canberra: Australian Government, 2013), 39, http://dfat.gov.au/about-us/publications/international-relations/australian-safeguards-non-proliferation-office-annual-report-2012-2013/pdf/dfat_asno_annual_report_1213.pdf.

17. International Panel on Fissile Materials (IPFM), *Global Fissile Material Report 2013: Increasing Transparency of Nuclear Warhead and Fissile Material Stocks as a Step toward Disarmament* (Princeton, NJ: IPFM, 2013), 24–25, http://fissilematerials.org/library/gfmr13.pdf.

18. In addition, a few countries, such as North Korea and India, have domestic suppliers.

19. On Iran, Pakistan, and North Korea, see International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A. Q. Khan and the Rise of Proliferation Networks: A Net Assessment* (London: International Institute for Strategic Studies, 2007), chaps. 2–3. On India, 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. On Brazil, see Mark Hibbs, "Ex-MAN Gas Centrifuge Expert Said Higher-Ups Helped Iraq," *Nuclear Fuel* 23 (6) (March 23, 1998): 5.

20. Scott R. Kemp, "The Nonproliferation Emperor Has No Clothes," *International Security* 38 (4) (April 2014): 39–78, http://dspace.mit.edu/openaccess-disseminate/1721.1/89182.

dollars.[21] Where reactor technology is concerned, the incentives for legal trade include not simply reduced costs but huge advantages in safety and reliability.

Against this background, advanced nuclear nations have adopted three basic strategies toward the development and trade of new nuclear technologies:[22]

- **Develop and deny.** A state chooses to develop a technology but refuses to transfer it. The United States applied this strategy to all nuclear technology between the passage of the MacMahon Act in 1946 and the passage of Atomic Energy Act of 1954.
- **Develop and disseminate.** A state develops a technology and then sells it subject to conditions (such as international monitoring) designed to prevent it from being used for proliferation. The United States has applied this strategy to light water reactors since they were first commercialized in the 1950s.
- **Desist and discourage.** A state refrains from developing a specific sensitive nuclear technology and encourages others to adopt similar restraint. The United States has adopted this strategy with regard to reprocessing for most of the period since 1976, when President Gerald Ford first announced a temporary moratorium on domestic reprocessing, which was extended indefinitely by President Jimmy Carter the following year.

As the examples illustrate, states do not necessarily apply the same strategy to different technologies. Moreover, these strategies are "ideal" types; in practice, the lines between them may be blurred. For example, although the United States has a policy against reprocessing, it nonetheless conducts basic research in this area. The Urenco states, meanwhile, have a general policy against selling enrichment technology but have made exceptions for the United States and France, while Russia, which has a similar basic policy, made an exception for China.

A third critical component of dual-use controls is the international oversight of domestic nuclear activities—known as safeguards—to detect and deter their use for military purposes. Safeguards, which in most cases are administered by the IAEA, are integral to the effectiveness of a develop-and-disseminate strategy but may also be needed under a develop-and-deny strategy if the developer has pledged not to develop nuclear weapons (centrifuge programs in Germany, the Netherlands, and Japan are examples of this latter case).

One characteristic of uranium or plutonium that facilitates safeguards is that their quantity (more properly, the mass of any given isotope) is conserved

21. For a somewhat dated cost estimate of Iran's enrichment program (which is scaled to military ends), see Thomas W. Wood, Matthew D. Milazzo, Barbara A. Reichmuth, and Jeffrey Bedell, "The Economics of Energy Independence for Iran," *Nonproliferation Review* 14 (1) (March 2007): 92, http://www.nonproliferation.org/wp-content/uploads/npr/141wood.pdf.

22. James M. Acton, "Nuclear Power, Disarmament and Technological Restraint," *Survival* 51 (4) (August–September 2009): 105–108, 111–115.

except in a nuclear reactor.[23] For example, in an enrichment plant, the quantity of uranium-235 in the feedstock must be equal to the sum of the quantities in the product and waste streams. This property permits an oversight process termed "material accountancy" in which inspectors take periodic inventories of declared nuclear materials, while also verifying declared transfers into and out of a facility. In theory, any discrepancy between the amount of material that is present and the amount that ought to be present indicates that the state has diverted nuclear material. In practice, this process is complicated by both unavoidable uncertainties in measurement and the practical impossibility of verifying all declared nuclear materials in most states, thus forcing inspectors to rely on sampling techniques to verify only some fraction of it. As a result, inspectors can provide only statistical, and not absolute, confidence in nondiversion.[24] For decades, material accountancy and IAEA safeguards were virtually synonymous. Although safeguards have now expanded significantly in scope, material accountancy still occupies a central role.

Neither material accountancy nor any of the other safeguards activities that now complement it can, however, physically prevent a state from using nuclear material or facilities in the development of nuclear weapons (only military force creates even the possibility of achieving that). Rather, the primary purpose of safeguards is deterrence by threatening to expose would-be proliferators as early as possible (as such, safeguards are often compared to burglar alarms rather than to door locks).[25] Whether this strategy is likely to be successful depends on both the perceived probability of being caught and the expected consequences. For this reason, the capability and willingness of not only the international community as a whole but of individual members to impose costs on states that violate their nonproliferation obligations is integral to the ultimate effectiveness of international oversight efforts.

At a conceptual level (if not an operational level), nuclear security efforts are significantly simpler than nonproliferation for two basic reasons. First, much of the complexity of nuclear nonproliferation stems from efforts to allow states access to inherently sensitive technology but to restrict the purposes for which it can be employed—a problem that does not arise with nuclear security, where the goal is to deny unauthorized use entirely. Second, nonstate actors, the primary "target" of nuclear security efforts, are significantly less capable than states.

23. Nuclear materials are radioactive and decay, but the relevant timescale is typically so long that decay can be ignored. Moreover, predicting how much of a bulk sample will decay in any given period of time is straightforward, with no meaningful uncertainty.

24. The IAEA's safeguards goals are given in IAEA, *IAEA Safeguards Glossary*, 24. For a more comprehensive discussion, see Rudolf Avenhaus and Morton John Canty, *Compliance Quantified: An Introduction to Data Verification* (Cambridge: Cambridge University Press, 1996), chap. 7.

25. The IAEA's Model Comprehensive Safeguards Agreement explicitly states that "the objective of safeguards is the timely detection of diversion of . . . nuclear material . . . and deterrence of such diversion by the risk of early detection." IAEA, *The Structure and Content of Agreements between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons*, INFCIRC/153 (corrected) (Vienna: IAEA, 1972), para. 28, http://www.iaea.org/sites/default/files/publications/documents/infcircs/1972/infcirc153.pdf.

Academics have extensively debated whether nonstate actors could build a viable nuclear weapon if they acquired sufficient weapon-usable nuclear material.[26] However, most would agree that nonstate actors lack the capacity to manufacture fissile material themselves.

Accordingly, nuclear security is focused on preventing nonstate actors from acquiring nuclear material. (Keeping information or equipment that could be used to manufacture fissile material, such as components for enrichment facilities, out of the hands of nonstate actors is also important, although the aim here is largely to prevent such information and equipment from then being sold to states. As such, this tends to be classed as a nonproliferation measure.) Physical protection measures—to deny unauthorized access to nuclear material and facilities—are the most important nuclear security measures. However, because of the potential consequences of failures in physical security, best practice demands multiple layers of protection, an approach known as "defense in depth." Other layers include efforts to detect the theft of material (such as material accountancy) and strategies for locating and recovering stolen material rapidly. Nuclear forensics, which can help determine the origin of recovered nuclear material, can expose security breaches and thus provides an incentive for states to secure nuclear materials properly. Deterrence may play a secondary role to prevention insofar as nonstate actors may be deterred from even attempting to acquire nuclear material if they believe failure is sufficiently likely. Threats to punish those involved in nuclear terrorism may also play some role, albeit probably only a marginal one (especially if the would-be terrorists are suicidal). Potential financers of a terrorist organization, for example, may have "something to lose" and so can perhaps be deterred from providing assistance by the threat of punishment.[27] Preventing terrorist organizations from gaining access to nuclear material is, however, unquestionably preferable to relying on deterrence or attempting to recover stolen material.

INTERNATIONAL REGULATION OF NUCLEAR TECHNOLOGY

Nuclear nonproliferation and nuclear security are not only conceptually distinct; the international systems to promote them are largely separate. Almost all relevant international institutions and agreements are concerned with one or the other but not both. The IAEA is the exception that proves the rule, since its nonproliferation and nuclear security functions have a "firewall" between

26. See, for example, John Mueller, *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al Qaeda* (Oxford: Oxford University Press, 2010), 172–176; and Anna M. Pluta and Peter D. Zimmerman, "Nuclear Terrorism: A Disheartening Dissent," *Survival* 48 (2) (Summer 2006): 55–69.

27. Lewis A. Dunn, *Can Al Qaeda Be Deterred from Using Nuclear Weapons?* Occasional Paper 3 (Washington, D.C.: Center for the Study of Weapons of Mass Destruction, National Defense University, July 2005), 8, http://wmdcenter.dodlive.mil/files/2005/07/03_Alqaeda_Nuclear_Weapons.pdf.

them. Inspectors, for example, may not officially report on any weaknesses in nuclear security they observe during safeguards inspections.[28] Moreover, the two systems are structured very differently. The nonproliferation regime is a relatively comprehensive system based largely on legally binding agreements. By contrast, the nuclear security architecture—even the term "regime" seems inappropriate—is a patchwork of arrangements, most of which are not legally binding, containing many omissions. One important consequence of this difference is that domestic nonproliferation requirements tend to vary much less between states than domestic nuclear security requirements.

These structural differences reflect differences in where states believe the responsibility for nonproliferation and nuclear security should lie. For decades, preventing the spread of nuclear weapons has widely been seen as an international task. Even if states disagree intensely about how to go about this task, the very fact that it is viewed as a collective responsibility has facilitated the creation of a comprehensive and legally binding system. By contrast, nuclear security was originally seen as an exclusively domestic matter and even today is still largely seen in those terms. As a result, the nuclear security architecture has been accreted over time, resulting in a patchwork. One indication of the difference is that the United States and its partners are regularly criticized for failing to show sufficient deference to international institutions on nonproliferation, whereas they are criticized for being too heavy handed in interfering with sovereign affairs where nuclear security is concerned.

Why the international community takes such different approaches to nuclear nonproliferation and nuclear security is not at all obvious—or rather, it is not obvious why nuclear security is not regarded as a matter for a comprehensive and legally binding international oversight regime. After all, internationally, nuclear security is *less* controversial than nonproliferation, and all states would probably agree that it is a global public good (even if many developing states would also argue that the threat from nuclear terrorism has been exaggerated). The answer may be, in part, historical. The nonproliferation regime originated in the Cold War, and its creation was made possible by the existence of two superpowers and their willingness to cooperate, not least by strong-arming recalcitrant allies into pledging not to acquire nuclear weapons. At the time, nuclear proliferation was (rightly, in my opinion) viewed as a much greater threat than nuclear terrorism, which presumably explains why the superpowers chose to focus on it. Moreover, a natural quid pro quo could be made: under the terms of the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), non-nuclear-weapon states (defined as those that had not exploded a nuclear weapon prior to January 1, 1967) promised not to acquire nuclear weapons in return for a commitment—by all states—to work in good faith toward nuclear disarmament. By contrast, a comprehensive nuclear security treaty would probably have required the United

28. Wyn Q. Bowen, Matthew Cottee, and Christopher Hobbs, "Multilateral Cooperation and the Prevention of Nuclear Terrorism: Pragmatism over Idealism," *International Affairs* 88 (2) (2012): 349.

States and the Soviet Union to accept international oversight of their domestic nuclear activities, an outcome they would have found far more disagreeable than the NPT's disarmament promise, which was described at the time by a U.S. official, who later became head of the Arms Control Association, as "an essentially hortatory statement" that "presents no problems."[29]

Although concern about nuclear terrorism occasionally surfaced during the Cold War, not until the terrorist attacks of September 11, 2001 was the issue firmly placed on the international agenda. However, international consensus on the severity of the threat has been hard to come by. Many non-Western states worry much more about being subject to burdensome regulations and being denied access to nuclear technology than they do about nuclear terrorism.[30] Moreover, the end of the bipolar international system and changes in U.S. domestic politics that make treaty ratification much more difficult have severely complicated the negotiation and implementation of international treaties. Collectively, these factors have militated against the "internationalization" of nuclear security.

The International Nuclear Nonproliferation Regime

The seeds of the nuclear nonproliferation regime were sown in 1953 when President Dwight Eisenhower announced in his "Atoms for Peace" speech at the United Nations (UN) that the United States was willing to share nuclear materials and technology (in the terminology of this article, he announced a switch from a develop-and-deny strategy to a develop-and-disseminate strategy), and proposed the creation of the International Atomic Energy Agency (IAEA). Eisenhower originally conceived the IAEA's primary function as receiving and allocating military-origin fissile materials donated by nuclear-armed states—a task it did not end up fulfilling. But, the IAEA Statute (the treaty, concluded in 1956, that created the agency and governs its operations) entrusted it with applying safeguards to bilateral nuclear trade agreements at the request of the contracting parties—the origin of its safeguards role. Today, such "item-specific" safeguards (also known as INFCIRC/66 safeguards after the IAEA information circular setting out their terms) are in force for nuclear facilities acquired by trade in three of the states that never signed the NPT: India, Israel, and Pakistan.

Eisenhower's approach marked a change of course for the United States, which seven years earlier had explicitly rejected the whole idea of safeguards. In 1946, the Acheson-Lilienthal report, which informed the first American

29. Spurgeon Keeny, memorandum for Henry Kissinger, "Provisions of the NPT and Associated Problems," January 24, 1969, 5, in U.S. Department of State Archive, http://2001-2009.state.gov/documents/organization/90727.pdf.

30. Bowen, Cottee, and Hobbs, "Multilateral Cooperation and the Prevention of Nuclear Terrorism," 354–356; and Jack Boureston and Tanya Ogilvie-White, "Seeking Nuclear Security through Greater International Coordination" (working paper, Council on Foreign Relations, March 2010), 13–14, http://www.cfr.org/content/publications/attachments/IIGG_WorkingPaper_1_NuclearSecurity.pdf.

proposal for the control of atomic energy, the Baruch Plan, had concluded that "there is no prospect of security against atomic warfare in a system of international agreements to outlaw such weapons controlled only by a system which relies on inspection and similar police-like methods."[31] The subsequent volteface seems to have had much more to do with Cold War grand strategy than any fundamental reassessment of the report's conclusions. Although extraordinarily prescient, the report had its weaknesses. Most notably, its authors focused only on the impossibility of using "inspection and similar police-like methods" to *prevent* proliferation and not on the possibility that they might be able to *deter* it—which was odd because the report did argue that deterrence would help enforce its preferred solution, an agreement to internationalize the fuel cycle.[32]

The conclusion of NPT in 1968 marked the next key moment in the development of the nuclear nonproliferation regime. To try to stem proliferation while allowing states access to dual-use nuclear technology, the NPT requires all non-nuclear-weapon states to accept IAEA safeguards on all their nuclear activities. To compensate for the inequality of the resulting two-tier system of nuclear-weapon states and non-nuclear-weapon states, the treaty also contains a disarmament commitment (in article VI) along with a separate commitment (in article IV) that requires "the fullest possible exchange" of nuclear materials, equipment, and knowledge between states.

IAEA safeguards, which were subsequently elaborated in INFCIRC/153, also known as the Model Comprehensive Safeguards Agreement, are primarily focused on detecting the diversion of nuclear material (plutonium, enriched uranium, or uranium-233) from declared facilities.[33] To this end, states are required to submit comprehensive reports on their holdings of nuclear materials, which the IAEA then verifies through material accountancy. INFCIRC/153 places no limits on what nuclear activities states are permitted to conduct, so long as all nuclear materials are declared and inspected. (Most states would argue that the NPT's only restriction on non-nuclear-weapon states is its prohibition against the "manufacture" of nuclear weapons—an injunction of unclear meaning—and that they have an "inalienable right" to conduct any other nuclear activity,

31. Chester I. Barnard, J. R. Oppenheimer, Charles A. Thomas, Harry A. Winne, and David E. Lilienthal, *A Report on the International Control of Atomic Energy* (Washington, D.C.: U.S. Government Printing Office, March 1946), 4, available from http://www.learnworld.com/ZNW/LWText.Acheson-Lilienthal.html.

32. Ibid., 61.

33. A voluntary reporting scheme for separated neptunium and americium was established in 1999 but is apparently barely used.

however sensitive.[34] The U.S. government and some U.S. scholars take a more restrictive view.[35])

Although INFCIRC/153 requires states to safeguard *all* their nuclear activities—and hence gives the IAEA the legal right to investigate undeclared activities—it does not provide the agency with sufficient tools to draw credible conclusions in that regard, presumably because, at the time the document was drafted, fissile material production was believed to be such a large-scale enterprise that it could not be successfully hidden. This assumption was shown (rather spectacularly) to be false in 1991 when, following the Gulf War, Iraq's clandestine nuclear weapons program was discovered.

In response the IAEA sought both to use its existing legal powers more fully (by, for example, making use of open-source information) and to develop an enhanced safeguards document with new legal powers, the Model Additional Protocol, INFCIRC/540.[36] This document, which was endorsed by the IAEA's Board of Governors in 1997, contains some "housekeeping" items, such as requiring states to provide inspectors with multiple-entry visas, but its key provisions are (1) expanded declarations by states, including about activities not involving nuclear material; and (2) much greater access rights for the IAEA, including outside of declared nuclear facilities and at short notice. In states with an additional protocol in force, the IAEA attempts to draw a "broader conclusion" that not only has no declared nuclear material been diverted but also that no undeclared material exists in the state. In 2014, 118 out of the 184 non-nuclear-weapon states party to the NPT had an additional protocol in force (as does Taiwan), and the broader conclusion had been drawn in sixty-five of them.[37] Of the sixty-five without an additional protocol in force, eleven conduct significant nuclear activities.[38] Two of these states, Iran and Syria, were in noncompliance with their safeguards agreements (though Iran has subsequently returned to compliance), while a number of the others, including Algeria and Egypt, are regarded as potential proliferators.

In addition to legal reform, a separate—and more controversial—wave of on-going organizational and conceptual reform is underway. Traditionally, the

34. On the meaning of the prohibition against manufacturing nuclear weapons, see James Acton with Carter Newman, *IAEA Verification of Military Research and Development*, Verification Matters 5 (London: VERTIC, 2006), 13–14, http://www.vertic.org/media/assets/Publications/VM5.pdf.

35. For example, Christopher Ford, "Statement to the 2005 Review Conference of the Treaty on the Nonproliferation of Nuclear Weapons, New York, New York," May 18, 2005, in U.S. Department of State Archive, http://2001-2009.state.gov/t/vci/rls/rm/46604.htm.

36. For a discussion of the IAEA's legal authority, see IAEA, *The Safeguards System of the International Atomic Energy Agency* (Vienna: IAEA, n.d.), 4–6, http://web.archive.org/web/20140104152301/http://www.iaea.org/safeguards/documents/safeg_system.pdf.

37. IAEA, *IAEA Annual Report 2014* (Vienna: IAEA, 2015), 100, https://www.iaea.org/sites/default/files/gc59-7_en.pdf.

38. These are Algeria, Argentina, Belarus, Brazil, Egypt, Iran, Malaysia, Serbia, Syria, Thailand, and Venezuela. Australian Safeguards and Non-Proliferation Office, *Annual Report 2012–13*, 106.

IAEA has looked at each facility in a state as an isolated entity and attempted to verify that no diversion from it has occurred. Then, in the early 2000s, the agency started to implement the "state-level approach," in which it holistically examines "all nuclear material, nuclear installations and nuclear fuel cycle related activities" in a state to try to draw conclusions about the absence of undeclared activities.[39] It initially focused on implementing this approach in those states with an additional protocol in force, but now does so in some states without one. In a closely related (some would say, inseparable) development, the IAEA has also moved to diversify the range of information sources available to it, under an approach termed "information-driven safeguards." In addition to information supplied by states in declarations and obtained by inspectors, the agency now makes regular use of open-source information, commercial satellite imagery, and intelligence information supplied by member states. The IAEA has also sought to effect a change in organizational culture from an inspectorate of (nuclear material) accountants to one made up of detectives.

These changes proved controversial, although some aspects were simply the institutionalization of existing practice.[40] The IAEA's first publicly known use of intelligence information, for example, appears to have been in 1991 during its investigation of Iraq's nuclear program, when the United States supplied photographs from a military reconnaissance satellite, thus also marking the IAEA's first-known use of satellite imagery (albeit on a noncommercial basis). Open-source information was approved for use a few years later and was cited by the IAEA in its investigations into safeguards irregularities in South Korea in 2004 and Egypt in 2005. The agency also regularly referenced open-source information during its decade-long investigation into Iranian noncompliance.

In spite of this history, the debate over the state-level approach and information-driven safeguards has recently become much more acrimonious. Since 2012, Russia and other states, mostly from the Non-Aligned Movement (a grouping, originating in the Cold War, of states that were not aligned with either superpower), have started to question the state-level approach vociferously and to argue that it needs political approval from the IAEA Board of Governors.[41] One worry is that, under the state-level approach, the choice of safeguards measures for a state depends on "state-specific factors" such as

39. IAEA, *IAEA Safeguards Glossary*, 19.

40. A summary of the use of open-source information, satellite imagery, and intelligence information by the IAEA is provided in James M. Acton, "International Verification and Intelligence," *Intelligence and National Security* 29 (3) (2014): 345–346, 348–350.

41. Mark Hibbs, "The Plan for IAEA Safeguards," Carnegie Endowment for International Peace, November 20, 2012, http://carnegieendowment.org/2012/11/20/plan-for-iaea-safeguards/ekyb#.

the "state's legal framework for implementing safeguards obligations."[42] The agency argues that this approach allows "differentiation without discrimination," whereas critics appear to worry that differentiation automatically constitutes discrimination.[43] Moreover, given that the agency's ultimate goal is to apply the state-level approach (or at least some elements of it) in all states, concerns have been raised, in particular by Brazil and Argentina, that the IAEA is attempting to force states that have not adopted an additional protocol into implementing some of its provisions.

Russia, meanwhile, has led the charge against the use of intelligence information. The agency's reports on Iran incorporated such information, which was provided largely—if not exclusively—by a small number of Western states, to an unprecedented degree. Moscow worries that this practice could enable the suppliers—the United States, in particular—to deliberately mislead the agency and justify military action.[44] The IAEA counters this objection by arguing that information supplied by member states is used only where it can be corroborated by other sources and represents just a small fraction of the total available information. However, given U.S. and British intelligence failures in the run-up to the Iraq War in 2003, the Russian argument has struck a chord internationally. Russian concerns also tie into a broader "fairness narrative" about the undemocratic way the agenda of international institutions is set by a small number of rich nations.

Western and other like-minded nations are not particularly satisfied with the status quo either, but their discontent stems from weaknesses in the safeguards system. In spite of the considerable improvement in safeguards since 1991, the intrinsically difficult task of detecting undeclared facilities—particularly small gas-centrifuge enrichment plants—almost certainly remains the agency's biggest technical challenge (although material accountancy in large, bulk handling facilities is also difficult). While no silver bullet has been found for this or any other problem, plenty of ideas for improving the effectiveness of safeguards have been proposed. Few of them have been implemented recently, however, because most meaningful improvements to safeguards require the approval of the thirty-five-member IAEA Board of Governors, which is rarely forthcoming. To give but one example, the Model Additional Protocol requires adherents to report on exports and imports of specified types of equipment and nonnuclear materials. To facilitate updates, the list setting out which transfers must be reported was included in an annex to the Model Additional Protocol that can be amended by the Board of Governors and without the consent of every

42. Jill N. Cooley, "Progress in Evolving the State-Level Concept" (paper presented at the 7th INMM/ESARDA Joint Workshop on Future Directions for Nuclear Safeguards and Verification, Aix-en-Provence, France, October 17–20, 2011), 4, http://www.inmm.org/AM/Template.cfm?Section=Evolving_the_IAEA_State_Level_Concept&Template=/CM/ContentDisplay.cfm&ContentID=2965.

43. Ibid., 3.

44. Hibbs, "The Plan for IAEA Safeguards."

signatory. To date, however, the board has not even considered proposals to update the annex.

An almost inevitable corollary to the nuclear nonproliferation regime's greatest strengths—its legally binding nature and near universality—is that reform is slow and difficult, since permission from so many participants is required. States opposed to reform offer a variety of objections. Some are technical, such as a desire to protect commercially sensitive information or the concern that enhanced safeguards might interfere with the smooth running of nuclear facilities. However, the most commonly heard objection, offered in particular by states in the Non-Aligned Movement, is that nuclear-weapon states, by not disarming, have failed to live up to their side of the NPT bargain and that, until they do disarm, a focus on further enhancing the nonproliferation regime is unfair.

That said, for all the challenges facing the international nonproliferation regime today, IAEA safeguards still represent a remarkable innovation. The use of intrusive international inspections at highly sensitive facilities to monitor dual-use technology was unprecedented. In fact, the very idea of safeguards runs counter to traditional notions of Westphalian sovereignty and was dismissed on realist grounds by the otherwise decidedly idealistic framers of the Acheson-Lilienthal report. Even today, only one directly comparable arrangement is in force: inspections and monitoring pursuant to the 1993 Chemical Weapons Convention to ensure that chemical production facilities are not used to produce prohibited agents. (Onsite inspections have also been facilitated by various arms limitation treaties—including those that are currently taking place under the terms of the New Strategic Arms Reduction Treaty, or New START—but the goal there is to verify limits on military capabilities, not to detect the employment of dual-use facilities for military ends.)

Overall, it is difficult to argue that IAEA safeguards have not played an important role in ensuring that the spread of nuclear weapons has been much slower than the spread in nuclear technology. To be sure, the IAEA's failure to detect Iraq's clandestine nuclear program prior to 1991 was a profound embarrassment—but, to be fair, the IAEA never claimed the inspection authority it had at the time would allow it to uncover such a program. Moreover, as the Acheson-Lilienthal report predicted, states have sometimes denied access to inspectors, lied to them, or otherwise inhibited their operation. However, poor cooperation in Iran, North Korea, and Syria did not prevent inspectors from presenting enough evidence that these states had violated their safeguards agreements so that the Board of Governors could make a formal finding of noncompliance.

Each of those findings provided meaningful warning of a real proliferation risk—even if the international community subsequently failed to use this warning effectively. Although the agency's investigation into Syria began only after its plutonium-production reactor had been destroyed by Israel in 2007,

it did highlight the risk that other undeclared facilities might remain.[45] North Korea was first found in noncompliance in 1994, and Iran in 2005, before either had developed a nuclear weapon. None of these cases has been satisfactorily resolved. Syria has still not provided access to the suspect facilities, and North Korea tested its first nuclear weapon in 2006. More positively, an agreement with Iran, the Joint Comprehensive Plan of Action, commonly known as the "Iran nuclear deal," was reached in July 2015 and entered into force in October 2015. Whether this agreement will prove successful is not yet clear (though, as of this writing in March 2016, implementation has proceeded smoothly).

The deal requires Iran to accept stringent restrictions on its nuclear program, most of which last for ten or fifteen years, as well as enhanced IAEA safeguards, in return for sanctions relief. The restrictions include a requirement to redesign the partially built heavy water reactor at Arak in order to curtail its ability to produce weapon-grade plutonium; limits on centrifuge numbers and types; limits on stockpiles of LEU; and limits on the level to which Iran can enrich uranium. At least some of the provisions represent genuine firsts in the management of dual-use nuclear technology, even if they have attracted less attention. For example, the deal extends IAEA monitoring, for the first time, to uranium mines and to the production and storage of centrifuge components. It obliges Iran to seek approval before importing specified dual-use equipment and materials. And it prohibits Iran from conducting specified activities that would be useful for designing or manufacturing a nuclear warhead. In all, this agreement offers a genuine prospect of resolving the Iran nuclear standoff. Full implementation will, however, take decades and is likely to prove difficult, not least because of potential domestic spoilers in both Tehran and Washington.

The failure to respond effectively to North Korean and Syrian noncompliance and the time required to find a credible pathway to resolving the Iranian crisis suggest that the biggest challenge facing the nonproliferation regime is not detecting violations but responding to them—or, as Fred Iklé once stated, "after detection—what?"[46] Even agreeing that a state has violated its nonproliferation commitments can be highly controversial. On at least two occasions, states that committed significant safeguards violations were "let off" without even a noncompliance finding: South Korea in 2004 and Egypt in 2005.[47] In the former case, which was more serious, the United States worked hard to shield its close ally. Initially at least, even finding Iran in noncompliance was met with opposi-

45. IAEA, *Implementation of the NPT Safeguards Agreement in the Syrian Arab Republic*, GOV/2011/30 (Vienna: IAEA, May 24, 2011), https://www.iaea.org/sites/default/files/gov2011-30.pdf.

46. Fred Charles Iklé, "After Detection—What?" *Foreign Affairs* 39 (2) (January 1961): 208–220.

47. IAEA, *Implementation of the NPT Safeguards Agreement in the Arab Republic of Egypt*, GOV/2005/9 (Vienna: IAEA, February 14, 2005), http://www.globalsecurity.org/wmd/library/report/2005/egypt_iaea_gov-2005-9_14feb2005.pdf; and IAEA, *Implementation of the NPT Safeguards Agreement in the Republic of Korea*, GOV/2004/84 (Vienna: IAEA, November 11, 2004), http://www.globalsecurity.org/wmd/library/report/2004/rok-gov-2004-84_iaea_11nov04.pdf.

tion. The IAEA had collected sufficient evidence by November 2003 to merit a noncompliance finding, but the process was delayed for two years because of concerns that it would disrupt negotiations and provide a justification for U.S. military action.

The NPT, the IAEA Statute, and the various safeguards agreements do not give any indication about how to respond to cases of noncompliance beyond stating that the IAEA Board of Governors should refer them to the UN Security Council, which achieved its greatest nonproliferation success following the 1991 Gulf War when it authorized and subsequently provided political backing for an exceptionally intrusive investigation into Iraq's nuclear, chemical, and biological weapons programs. Since then, however, the Security Council has been largely ineffectual, as the North Korean and Syrian cases demonstrate—although the Iranian case gives more cause for optimism. A discussion of what the Security Council could have done differently to facilitate resolution of these "hard cases" is beyond the scope of this paper. However, few would disagree that its effectiveness is currently limited by the inability of its members—particularly the veto-wielding states—to agree quickly on whether a case of noncompliance is a real problem and, if it is, what they should do about it.

Strategic trade or export controls are an important complement to IAEA safeguards. In fact, the safeguards system itself has some provisions related to international trade. INFCIRC/153 requires reporting of imports or exports of nuclear material, and the Model Additional Protocol requires states to inform the IAEA about transfers of certain types of equipment and nonnuclear material. These requirements are, however, not really controls, as they do not impose actual limitations.

Two multilateral arrangements—the Zangger Committee and the Nuclear Suppliers Group—go further and place some restrictions on transfers. Article III.2 of the NPT prohibits international transfers of nuclear material or "equipment or material especially designed or prepared for the processing, use or production of" nuclear material, unless safeguards are applied. To facilitate the implementation of this article, the Zangger Committee, an informal coalition that first met in 1971 and currently consists of thirty-eight states, has produced a "trigger" list of materials and equipment that participants agree the article covers.[48] Participating states agree that the supply of trigger list items should be subject to a set of minimal conditions that reflect the NPT's requirements, such as the application of IAEA safeguards and a pledge from the recipient not to use the material or equipment for the manufacture of nuclear weapons.

The Nuclear Suppliers Group, which was formed after India's "peaceful nuclear explosion" in 1974 and today has forty-six participating governments, is more ambitious than the Zangger Committee in two respects. First, it pub-

48. The trigger list is circulated by the IAEA as INFCIRC/209. The most recent version is IAEA, *Communication of 29 May 2014 Received from the Permanent Mission of Canada Regarding the Export of Nuclear Material and of Certain Categories of Equipment and Other Material*, INFCIRC/209/Rev.3 (Vienna: IAEA, June 19, 2014), https://www.iaea.org/sites/default/files/infcirc209r3.pdf.

lishes not only its own trigger list but a separate list of dual-use items (equipment that has both nuclear and nonnuclear applications).[49] Second, the group's guidelines impose somewhat more stringent conditions on transfers than the Zangger Committee. For example, the former requires recipients (except for nuclear-weapon states) to apply appropriate physical protection measures and to have safeguards on *all* their nuclear activities—although the United States persuaded the group to waive this latter requirement for India following the U.S.-India nuclear deal. Participating governments have also agreed to consider recipients' nuclear nonproliferation credentials before agreeing to transfers, and to exercise a "policy of restraint" toward transfers of enrichment and reprocessing technology.

Strategic trade controls, like others facets of the international nonproliferation regime, were revitalized following the discovery of Iraq's clandestine nuclear program in 1991 and, in particular, by the embarrassing revelation that it had sourced components for its centrifuges from Western companies. The Nuclear Suppliers Group, which had not met since 1978, subsequently became much more active and progressively tightened its guidelines. Its efforts, coupled to improved national export control programs, have almost certainly helped to slow the clandestine nuclear programs that have been discovered more recently. Moreover, since the UN Security Council passed Resolution 1540 in 2004, all states have been legally bound to implement export controls. Today, however, strategic trade controls face both technical and political challenges.[50]

A number of technical developments are conspiring to undermine the (already limited) effectiveness of trade controls and to complicate their implementation. Trade patterns are becoming more complex and increasingly involve middlemen, brokers, and transshipments, making them more difficult to monitor. An increasing number of states outside the Nuclear Suppliers Group are also involved (an estimated 110 states can now manufacture items on the group's dual-use list). Meanwhile, illicit trade has been facilitated by nonstate actors, most notably the network run by the Pakistani scientist A. Q. Kahn, which is believed to have been only partially dismantled. Perhaps most fundamentally, as Scott Kemp argues, would-be proliferators are increasingly able to get by without foreign assistance since "the technologies needed to make nuclear weapons have remained static, whereas the indigenous capabilities of states have steadily grown over the last half century."[51]

49. The trigger list and dual-use list are circulated by the IAEA as, respectively, parts 1 and 2 of INFCIRC/254. For the most recent versions see IAEA, *Communication Received from the Permanent Mission of the Czech Republic to the International Atomic Energy Agency Regarding Certain Member States' Guidelines for the Export of Nuclear Material, Equipment and Technology*, INFCIRC/254/Rev.12/Part 1 and INFCIRC/254/Rev.12/Part 2 (Vienna: IAEA, November 13, 2013), http://www.iaea.org/sites/default/files/publications/documents/infcircs/1978/infcirc254r12p1.pdf and http://www.iaea.org/sites/default/files/publications/documents/infcircs/1978/infcirc254r9p2.pdf.

50. Hibbs, *Future of the Nuclear Suppliers Group*.

51. Kemp, "The Nonproliferation Emperor Has No Clothes," 40.

The Nuclear Suppliers Group, in particular, also faces political challenges from within and from the outside. Its rules are nonbinding and have been violated, most notably by China in two recent agreements to supply Pakistan with reactors.[52] Decision-making is slow due to a need for consensus. Reaching agreement on tightening the rules for transfers of enrichment and reprocessing technology took more than seven years (and even then led to a distinctly unsatisfactory outcome).[53] Today, the Nuclear Suppliers Group has begun what promises to be a long and acrimonious process to decide on whether to admit India. Finally, what Mark Hibbs terms "the rise of international nuclear equity issues" has led to criticism of the group by non-nuclear-weapon states worried about becoming victims of export denials—a matter of importance not least because, while most of these states do not have nuclear power programs, some can manufacture sensitive components.[54]

The Nuclear Suppliers Group and the Zangger Committee might be described as "coalitions of the willing" that are multilateral but not truly international and impose politically but not legally binding rules on participants. Other such nonproliferation initiatives include the Proliferation Security Initiative and the Nuclear Power Plant Exporters' Principles of Conduct.

The Proliferation Security Initiative, which was launched in 2003 by the United States in cooperation with ten close allies, "aims to stop trafficking of weapons of mass destruction . . . their delivery systems, and related materials to and from states and non-state actors of proliferation concern" by interdicting dangerous cargoes in transit.[55] Initially, it proved highly controversial, not least because many states appeared to have the impression (contrary to what was actually written in the "Statement of Interdiction Principles") that it would involve illegally boarding ships on the high seas. Concerns have, however, gradually abated as, in practice, the initiative has focused on capacity building (including through exercises) and streamlining procedures for sharing information to help states enforce existing laws more effectively. Meanwhile, the United States has negotiated bilateral boarding agreements with eleven flag states in which

52. Mark Hibbs, "Power Loop: China Provides Nuclear Reactors to Pakistan," *Jane's Intelligence Review*, January 2014, 52–53, http://carnegieendowment.org/email/DC_Comms/img/JIR1401%20F3%20ChinaPak.pdf.

53. Fred McGoldrick, with Matthew Bunn, Martin Malin, and William H. Tobey, *Limiting Transfers of Enrichment and Reprocessing Technology: Issues, Constraints, Options* (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2011), 13–17, http://belfercenter.ksg.harvard.edu/files/MTA-NSG-report-color.pdf; and Mark Hibbs, "New Global Rules for Sensitive Nuclear Trade," *Nuclear Energy Brief*, Carnegie Endowment for International Peace, July 28, 2011, http://carnegieendowment.org/2011/07/28/new-global-rules-for-sensitive-nuclear-trade#.

54. Hibbs, *Future of the Nuclear Suppliers Group*, 11.

55. U.S. Department of State, "Proliferation Security Initiative," n.d., http://www.state.gov/t/isn/c10390.htm.

over 55 percent of the world's shipping (by tonnage) is registered.[56] A further 22 percent is registered with other initiative participants. Today, 102 states have endorsed the "Interdiction Principles," which is the only requirement for "membership"— although how many of these states participate actively is unclear.[57] Indeed, the effectiveness of the initiative is hard to assess, not least because participating states reveal little information about its activities.[58]

The Nuclear Power Plant Exporters' Principles of Conduct is a corporate and social responsibility code for nuclear reactor exporters and has been adopted by all the world's major vendors outside of China.[59] The Principles of Conduct are the most important example of a code of ethics for nuclear nonproliferation, albeit among corporations rather than individuals. They also cover more than nonproliferation; indeed, their most significant provisions relate to other issues, most notably safety. In large part, participants' nonproliferation commitments extend no further than abiding by existing national and international rules and assisting reactor recipients to meet their obligations, although vendors also commit, for example, to "promote proliferation-resistant [reactor] designs" and to inform national authorities "in a timely manner . . . of any serious nonproliferation concerns."[60] The Principles of Conduct illustrate a general difficulty of codes of conduct in the nuclear field: because there is so much national and international nonproliferation regulation, individuals and organizations tend to see their ethical responsibility purely in terms of complying with existing rules.

International Nuclear Security Efforts

Although promoting nuclear security, alongside safety and safeguards would have been a natural fit for the IAEA, the subject was not discussed during negotiations over the agency's founding and is not mentioned in its statute.[61] Not until 1972 did the agency carve out a role for itself in nuclear security by issuing—against initial opposition from a number of Western states—a set of nonbinding guidelines on nuclear security, INFCIRC/225, which has since

56. U.S. Department of State, "Ship Boarding Agreements," n.d., http://www.state.gov/t/isn/c27733.htm; and United Nations Conference on Trade and Development, *Review of Maritime Transport 2014* (New York: United Nations, 2014), 44–45, http://unctad.org/en/PublicationsLibrary/rmt2014_en.pdf.

57. Nuclear Threat Initiative, "Proliferation Security Initiative," 2015, http://www.nti.org/treaties-and-regimes/proliferation-security-initiative-psi/.

58. James R. Holmes and Andrew C. Winner, "The Proliferation Security Initiative," in Nathan E. Busch and Daniel H. Joyner, eds., *Combatting Weapons of Mass Destruction: The Future of International Nonproliferation Policy* (Athens: University of Georgia Press, 2009), 148–150. Holmes and Winner also observe that even defining success is highly problematic.

59. Nuclear Power Plant Exporters' Principles of Conduct, "Participants," n.d., http://nuclearprinciples.org/participants/.

60. *Nuclear Power Plant Exporters' Principles of Conduct*, March 6, 2014, 8, http://nuclearprinciples.org/wp-content/uploads/2014/03/PrinciplesofConduct_March2014.pdf.

61. David Fischer, *History of the International Atomic Energy Agency: The First Forty Years* (Vienna: IAEA, 1997), 229–230, http://www-pub.iaea.org/mtcd/publications/pdf/pub1032_web.pdf.

been revised five times.[62] Later in the decade, the agency took a leading role in preparing the first binding treaty on nuclear security, the 1980 Convention on the Physical Protection of Nuclear Material (CPPNM). This agreement focuses almost exclusively on materials in international transport and, like later nuclear security agreements, sets out steps that states must take to protect materials covered by the convention (by, for example, applying appropriate physical protection measures and criminalizing certain kinds of offenses). In contrast to the NPT, which assigns the IAEA a critical verification function, the only roles assigned to the agency by the CPPNM are purely administrative (for example, in sharing information about national points of contact, states may make use of the agency, though they are not required to do so). In a signal of the importance—or lack thereof—that states placed on nuclear security, seven years passed before the treaty garnered the twenty-one ratifications required for entry into force. Today 153 states are party to the CPPNM.[63]

In the 1990s, the IAEA acquired two other important nuclear security functions. First, following the collapse of the Soviet Union in 1991, detection of the smuggling of nuclear and radiological materials rose dramatically. The IAEA assisted in efforts to curtail such smuggling, most notably by creating the Illicit Trafficking Database in 1995 (although the agency had begun to collect media reports as early as 1992).[64] The agency also created the International Physical Protection Advisory Service to conduct peer review of states' nuclear security practices. These missions, which are initiated only at the request of states, have taken place since 1996.

Perhaps the most consequential international efforts prior to 2001, at least in terms of demonstrable results, were Soviet/Russian and, particularly, American bilateral programs with foreign partners. These efforts were initiated to mitigate a threat that the United States and Soviet Union had exported research reactors fueled with HEU.[65] In 1978, the United States launched the Reduced Enrichment Research and Test Reactor program to develop alternative LEU fuels for HEU-fueled research reactors and to undertake conversion of foreign reactors (the Soviet Union had an equivalent program). American nuclear security cooperation was dramatically stepped up in the early 1990s, facilitated in large part by the Nunn-Lugar Cooperative Threat Reduction program. The

62. The most recent version is IAEA, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, IAEA Nuclear Security Series no. 13, INFCIRC/225/Revision 5 (Vienna: IAEA, 2011), http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.

63. As of September 15, 2015. IAEA, *Convention on the Physical Protection of Nuclear Material* (Vienna: IAEA, September 15, 2015), https://www.iaea.org/Publications/Documents/Conventions/cppnm_status.pdf.

64. Fischer, *History of the International Atomic Energy Agency*, 120–122.

65. A slightly dated but comprehensive overview of efforts to mitigate this problem can be found in Frank von Hippel, "A Comprehensive Approach to Elimination of Highly-Enriched-Uranium from All Nuclear-Reactor Fuel Cycles," *Science & Global Security* 12 (2004): 137–164, http://scienceandglobalsecurity.org/archive/sgs12vonhippel.pdf.

scope of these efforts—which began with programs to reduce the risk from military and civilian nuclear materials in the former Soviet Union and were subsequently extended to include both chemical and biological threats, as well as other states—was vast. Two of the programs that originated at that time and are still ongoing are of particular note. First, the United States began efforts to take back both fresh and spent HEU fuel for U.S.-origin research reactors and worked with Russia to enable it to do the same for Soviet-supplied reactors. Second, in 1994, Washington set up the International Materials Protection and Cooperation program to help other states better secure nuclear materials and combat nuclear trafficking.

Since 2001, nuclear security initiatives have proliferated, even absent a broad consensus on the severity of the threat. Many of these efforts are not legally binding. In part, this reflects states' reluctance to cede sovereignty on nuclear security. However, it also reflects the proclivities of the administration of President George W. Bush, which had a visceral dislike of both legally binding international agreements and the slow pace of the diplomacy needed to negotiate them. Even the exceptions to this general state of affairs are revealing. Two of the legally binding instruments negotiated since 2001 are UN Security Council resolutions. Because these resolutions are negotiated among only fifteen states (of which just five have vetoes), they bypass many of the complexities of a truly international process. The administration of President Barack Obama has continued in largely the same vein, even though it is much more sympathetic to internationalism, in large part because the Bush administration's views are still alive and well in the Senate, which must provide its advice and consent to the ratification of treaties.

The measures that have originated since 2001 can be classified into five types: binding international law, nonbinding initiatives to facilitate cooperation, institutional reform, enhanced U.S. cooperation programs, and the sui generis Nuclear Security Summit process. The brief description that follows cannot do justice to the complexities and full scope of these multifaceted initiatives, activities, agreements, and organizations, and I unapologetically refer interested readers to a number of sources that provide the missing detail.[66]

Binding international law. Four legally binding instruments have been created since 2001. With the partial exception of the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), all focus nearly exclusively on the national implementation of measures to enhance nuclear security (as opposed, say, to mandating international cooperation):

66. For example, Boureston and Ogilvie-White, "Seeking Nuclear Security through Greater International Coordination"; Bowen, Cottee, and Hobbs, "Multilateral Cooperation and the Prevention of Nuclear Terrorism"; Centre for Science and Security Studies, King's College London, *Nuclear Security Briefing Book: 2014 Edition* (London: Centre for Science and Security Studies, King's College London, 2014), http://www.kcl.ac.uk/sspp/departments/warstudies/research/groups/csss/pubs/NSBB---Full-final.pdf; and Nuclear Threat Initiative, *Nuclear Security Primer: The Existing System* (Washington, D.C.: Nuclear Threat Initiative, September 2014), http://www.nti.org/media/pdfs/Nuclear_Security_Primer_September_2014.pdf?_=1413920986.

- UN Security Council Resolution (UNSCR) 1373 (2001) requires measures to suppress all forms of terrorism.
- UNSCR 1540 (2004) requires measures to prevent nonstate actors from acquiring or using nuclear, chemical, or biological weapons or their means of delivery (further resolutions have prolonged its mandate).
- The 2005 amendment to the CPPNM extends the treaty's jurisdiction to domestic nuclear materials.
- The 2005 ICSANT requires national legislation and international cooperation to prevent nuclear and radiological terrorism.

Voluntary initiatives to facilitate cooperation. Various "coalitions of the willing" have also been created to enable enhanced international cooperation on nuclear security:

- The G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction, created in 2002, funds projects to reduce the risk of nonstate actors acquiring nuclear, biological, chemical, or radiological material in both the former Soviet Union and, more recently, elsewhere.
- The Global Initiative to Combat Nuclear Terrorism, established in 2006, aims to promote best practice and strengthen international cooperation to deter, prevent, and respond to acts of nuclear terrorism.
- The Proliferation Security Initiative is unusual in serving both a nuclear security and nonproliferation role.

Institutional Reform. Greater support for national efforts to counter nuclear terrorism is now available through both new and existing institutions:

- The IAEA has enhanced its capacity to assist states with nuclear security by establishing the Office of Nuclear Security, which was recently upgraded to the Division of Nuclear Security. The agency also established a Nuclear Security Plan to guide its efforts and a Nuclear Security Fund to finance them through voluntary contributions.
- INTERPOL has improved its capacity to help prevent nuclear and radiological terrorism, including by enhanced cooperation with the IAEA.
- The World Institute for Nuclear Security has been established to promote best practice.
- Centers of excellence to provide training in nuclear security on a national and regional level have also been established by various countries.

Enhanced U.S. cooperation programs. The United States has also stepped-up its bilateral cooperation programs. Perhaps most important, in 2004 the Bush administration launched the Global Threat Reduction Initiative to convert both research reactors and the targets used in radioisotope production to enable their use of LEU rather than HEU; to remove excess nuclear and radiological materials; and to enhance the physical security of vulnerable

materials. (The initiative represented a consolidation and expansion of existing efforts.) This program was given a major boost in 2009 when Obama, during his Prague speech, articulated the goal of securing all vulnerable nuclear materials within four years. Although this target was not met, U.S. efforts were accelerated and have resulted so far in the removal or disposition, in some cases in cooperation with Russia, of nearly three thousand kilograms of HEU and plutonium from foreign states—more than doubling the total amount of material the United States has secured in this way.[67] As part of these efforts, the United States also imported, for the first time, both separated plutonium and non-U.S.-origin spent fuel.[68]

The Nuclear Security Summits. In his Prague speech, Obama also announced the first Nuclear Security Summit, which took place in Washington, DC, in 2010. Follow-up meetings were held in Seoul in 2012 and The Hague in 2014. A fourth, and almost certainly final, summit will be held in the United States in 2016. Although the summits do issue communiqués, their most important deliverables have been unilateral commitments, known colloquially as "house gifts" (a promise to facilitate the removal of HEU or plutonium to the United States or Russia is the diplomatic equivalent of a bouquet of flowers at these events). Such commitments are not actually negotiated by the heads of state at the summit—but the fact of the summit does force bureaucracies to make nuclear security a priority and to overcome long-standing barriers to progress, precisely so that their leaders can declare success at the meeting. The summits have also raised awareness of the issue, among both national leaders and (to a lesser extent) the general public.

Looking forward, perhaps the biggest question facing the nuclear security agenda is whether the momentum that has built up behind it is sustainable. With a few exceptions (such as the Proliferation Security Initiative in its early days), the nuclear security agenda is not all that controversial, at least in comparison to nuclear nonproliferation. In contrast, say, to adopting an additional protocol, few states evince a principled objection to ratifying the amendment to the CPPNM. Moreover, a few of the challenges to further progress in nuclear security are technical, including the need to develop new fuel designs so that reactors that still use HEU can be converted to use LEU. There is no reason to suppose these technical challenges will not eventually be overcome.

That being said, neither is there much sense of urgency, except from the United States and a few close partners. Almost ten years after being opened for signature, for example, the amendment to the CPPNM has still not entered into

67. U.S. Department of Energy, National Nuclear Security Administration, *The Four-Year Effort: Contributions of the Global Threat Reduction Initiative to Secure the World's Most Vulnerable Nuclear Material by December 2013*, YGG 13-0337 (Washington, D.C.: U.S. Department of Energy, 2013), 4, http://nnsa.energy.gov/sites/default/files/nnsa/12-13-inlinefiles/2013-12-12%204%20Year%20Effort.pdf.

68. Ibid., 5.

force.[69] In large part, the lack of urgency reflects the lack of shared perception of the threat. Moreover, simmering discontent from many non-nuclear-weapon states about the emphasis being placed on preventing nuclear terrorism—as opposed to, say, nuclear disarmament or technical assistance—has not dissipated and may have been increased by the high-level attention nuclear security has garnered.[70] All these factors raise doubts about sustainability.

To make matters worse, the nuclear security agenda can easily be derailed by unrelated political disputes. Russia, for example, has generally been supportive of nuclear security efforts. However, U.S.-Russian cooperation on nuclear security has now become a victim of the Ukraine crisis. In October 2014, Moscow informed Washington that it was not planning to attend the 2016 Nuclear Security Summit (preferring, it said, to support IAEA efforts).[71] More serious still, in December 2014, Moscow terminated cooperation with the United States on all nuclear security projects in Russia (though it has said it will continue cooperation focused on third countries).[72]

Moreover, U.S. leadership, which has often been instrumental to progress in nuclear security, should not be regarded as a given. While nuclear security is a "motherhood and apple pie" issue that no American politician opposes per se, it has little resonance with the public and is not generally seen as such a transcendently important issue that it should be immune from either budget cutbacks or partisanship. For a variety of reasons, including sequestration, the Obama administration has been gradually reducing its budget requests for nuclear security since fiscal year 2012.[73] In 2016, the Republican majorities in both the Senate and, particularly, the House of Representatives are likely to try to reduce actual spending yet further. Implementing legislation for ICSANT and the amendment to the CPPNM was, for a number of years, held hostage to an arcane and politicized domestic dispute over the death penalty and wiretapping (until such legislation is passed, the United States cannot deposit its

69. As of February 10, 2016, the amendment had been ratified by ninety-two states. For entry into force, two-thirds of states party to the treaty must ratify it. The current target is, therefore, 102—but this figure is liable to increase as more states ratify the convention. IAEA, *Amendment to the Convention on the Physical Protection of Nuclear Material* (Vienna: IAEA, February 10, 2016), https://www.iaea.org/Publications/Documents/Conventions/cppnm_amend_status.pdf.

70. Although slightly dated, this is highlighted throughout Boureston and Ogilvie-White, "Seeking Nuclear Security through Greater International Coordination."

71. Arshad Mohammed and Lidia Kelly, "Russia Told U.S. It Will Not Attend 2016 Nuclear Security Summit," Reuters, November 5, 2014, http://www.reuters.com/article/2014/11/05/us-nuclear-security-usa-russia-idUSKBN0IP24K20141105.

72. Bryan Bender, "Russia Ends U.S. Nuclear Security Alliance," *Boston Globe*, January 19, 2015, http://www.bostonglobe.com/news/nation/2015/01/19/after-two-decades-russia-nuclear-security-cooperation-becomes-casualty-deteriorating-relations/5nh8NbtjitUE8UqVWFIooL/story.html.

73. Matthew Bunn, Nickolas Roth, and William H. Tobey, *Cutting Too Deep: The Obama Administration's Proposals for Nuclear Security Spending Reductions* (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2014), http://belfercenter.ksg.harvard.edu/files/budgetpaper%20WEB.pdf.

instruments of ratification).[74] Meanwhile, the next U.S. president—whichever party he or she comes from—is unlikely to give nearly as much personal attention or time to the issue as Obama has, or continue the Nuclear Security Summit process (probably to the relief of many world leaders).

Sustainability matters both to avoid backsliding on the progress that has been made so far and to further enhance the nuclear security architecture, which currently has at least five key weaknesses.

First, it does not cover all nuclear materials—or even a majority of the most sensitive. About 85 percent of the HEU and separated plutonium in the world is military, and, now that U.S.-Russian cooperation on these materials has ended, they appear to be entirely exempt from the existing architecture, except for recognition in the communiqué from the 2014 Nuclear Security Summit of "the fundamental responsibility of States . . . to maintain at all times effective security of all nuclear . . . materials, including nuclear materials used in nuclear weapons."[75] What is more important for the present discussion, however, is that, while broad consensus exists on the desirability of minimizing civilian HEU use, no such agreement has been reached on civilian plutonium.[76]

Second, the standards mandated—or, in many cases, suggested—by existing agreements are often weak and, in some cases, ambiguous.[77] Such "watering down" is often necessary to ensure agreement among participating states.

Third, many initiatives are voluntary—in both senses of the word: states do not have to sign onto them, and the standards imposed are often not legally binding. The only legally binding measures that apply to all states are UN Security Council resolutions. All other binding instruments have limited participation. Meanwhile, no IAEA guidance on nuclear security is binding (although, at the 2014 Nuclear Security Summit, thirty-five nations did agree to abide by various agency recommendations).[78] Meanwhile, of the twenty-five states with

74. Matthew Bunn, "U.S. Failure to Ratify Key Nuclear Security Conventions," *Nuclear Security Matters,* March 12, 2014, http://nuclearsecuritymatters.belfercenter.org/blog/us-failure-ratify-key-conventions.

75. "Non-paper: Building International Confidence in the Security of Military Materials," Nuclear Threat Initiative, September 17, 2014, http://www.nti.org/analysis/articles/non-paper-building-international-confidence-security-military-materials/; and *The Hague Nuclear Security Summit Communiqué*, The Hague, March 25, 2014, para. 4, http://www.state.gov/documents/organization/237002.pdf.

76. The communiqué from the 2014 Nuclear Security Summit went no further than to "encourage States . . . to keep their stockpile of separated plutonium to the minimum level . . . as consistent with national requirements." *The Hague Nuclear Security Summit Communiqué*, para. 21.

77. Various examples are given in Boureston and Ogilvie-White, "Seeking Nuclear Security through Greater International Coordination," 2–9.

78. Algeria et al., *Joint Statement*, March 25, 2014, http://web.archive.org/web/20140326012847/https://www.nss2014.com/sites/default/files/downloads/strengthening_nuclear_security_implementation.pdf.

weapon-usable nuclear material, six have never invited a peer review of their security standards (and another has not done so within the past five years).[79]

Fourth, no nuclear security agreement has created a formal verification regime, and only a few have informal transparency provisions to enable states to demonstrate their compliance—and even those that do have met with only partial success. The most notable transparency arrangement was a requirement in UNSCR 1540 for states to submit reports, within six months of the resolution's adoption, detailing practices and plans for national implementation. Only fifty-one states met this deadline.[80] And by the time of the December 2014 annual review, twenty states had still failed to fulfill the requirement.[81] Moreover, among those reports that have been submitted, quality and comprehensiveness vary widely.

Fifth, the quality of national implementation of nuclear security measures appears to have been highly variable—although, in many cases, the available information is insufficient to enable an assessment.

In practice, correcting all these weaknesses simultaneously is probably impossible since the solutions to different problems can sometimes counteract one another. For example, if states tried to negotiate a verified, legally binding agreement on some aspect of nuclear security, they would probably end up with a document that was less demanding than existing voluntary standards (notably INFCIRC/225) and attracted a relatively limited number of signatories. A key question facing the nuclear security regime is, therefore, one of priorities; given the likely impossibility of making progress on all fronts simultaneously, on which of the weaknesses should energy be focused?

More broadly, one of the benefits of analyzing nuclear nonproliferation and nuclear security side by side is that it enables their strengths and weaknesses to be contrasted. The nonproliferation regime is comprehensive, nearly universal, and legally binding. However, changes are highly contested and, precisely because it is nearly universal, reform is painfully slow (absent crises, at least). By contrast, the nuclear security architecture is much more flexible. Some states choose to go faster than the pack and take on additional commitments (which is extremely unusual in nonproliferation). As a corollary, however, states that want to go slower are under relatively little pressure to do more. This comparison demonstrates that making the nuclear security regime more like the nonproliferation regime would not be a panacea. Comprehensiveness, universality,

79. Nuclear Threat Initiative, *NTI Nuclear Materials Security Index: Building a Framework for Assurance, Accountability, and Action*, 2d ed. (Washington, D.C.: Nuclear Threat Initiative, January 2014), 14, http://ntiindex.org/wp-content/uploads/2014/01/2014-NTI-Index-Report.pdf.

80. Lars Olberg, *Reporting to the 1540 Committee—A Snapshot* (New York: Lawyers Committee on Nuclear Policy, November 2005), 4, http://lcnp.org/disarmament/1540-olberg.pdf.

81. Oh Joon, "Letter Dated 31 December 2014 from the Chair of the Security Council Committee Established Pursuant to Resolution 1540 (2004) Addressed to the President of the Security Council," S/2014/958, United Nations Security Council, December 31, 2014, para. III.B.6, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2014/958.

legally binding standards, and verification could solve some problems, but at the expense of introducing others. The trade-offs involved are almost certainly relevant to other technologies.

U.S. DOMESTIC OVERSIGHT

The range of domestic nonproliferation and nuclear security oversight activities in the United States is vast. Major elements include:

- **Licensing** of civilian nuclear facilities and nuclear materials by the NRC. Although the primary function of licensing is ensuring safety, license conditions include requirements pertaining to physical security and the control and accountancy of nuclear materials.
- **Domestic nuclear security.** Licensees are responsible for implementing the security measures required by the NRC, which also verifies compliance.
- **Border security** to detect the illicit transport of nuclear material into the United States. These efforts, run by the Department of Homeland Security, include radiation detectors at U.S. ports of entry, as well as a program, the Container Security Initiative, to scan cargo bound for the United States at foreign ports.[82]
- **Voluntary IAEA safeguards** on nonmilitary facilities. Nuclear-weapon states party to the NPT are not required to accept IAEA safeguards. In 1977, however, the United States concluded a "voluntary offer" arrangement with the IAEA, under which it makes certain facilities available for safeguards. The U.S. "Eligible Facilities List" includes almost all facilities licensed by the NRC—GE Hitachi's pilot-scale laser enrichment facility is a notable exception—as well as about thirty Department of Energy facilities.[83] In practice, because of resource constraints, the IAEA has chosen to safeguard only a small number of these facilities and since 1994 has focused exclusively on storage facilities for materials declared to be in excess of military requirements.[84] Currently, just one facility, the

82. These programs are likely to be significantly more effective at detecting the smuggling of radioactive material, which is another of their goals.

83. The most up-to-date version of the NRC's portion of the Eligible Facilities List is available from NRC, "International Safeguards," last updated March 26, 2015, http://www.nrc.gov/about-nrc/ip/intl-safeguards.html. The Department of Energy does not make its list public. However, it does state that, in total, the United States makes "nearly 300" facilities available. Given that the most recent NRC list (from 2013) includes 261 facilities, the Department of Energy list must include about thirty facilities. U.S. Department of Energy, National Nuclear Security Administration, "NPT Compliance," n.d., http://nnsa.energy.gov/ourmission/managingthestockpile/nptcompliance.

84. IPFM, *Global Fissile Material Report 2007* (Princeton, NJ: IPFM, 2007), 72, http://fissilematerials.org/library/gfmr07.pdf.

K Area Material Storage Vault at Savannah River National Laboratory, is under IAEA safeguards.[85] The United States also has an additional protocol in force that contains the same provisions as the Model Additional Protocol except for a national security exemption. The NRC and the Department of Energy are primarily responsible for overseeing the implementation of these agreements, including by jointly operating a system for tracking U.S. nuclear materials.[86]

- **Domestic risk reduction efforts**, led by the Department of Energy, include the management and disposition of excess military fissile materials.
- **Nuclear cooperation agreements**, negotiated by the Department of State, permit international trade in nuclear materials and facilities.
- **Export controls** to prevent U.S. technology, material, and equipment from being obtained by non-U.S. entities that might misuse them. Licenses for nonmilitary nuclear exports are granted by three agencies: the NRC (nuclear materials, reactors, and certain key reactor components), the Department of Commerce ("outside the core" equipment for nuclear reactors), and the Department of Energy (nuclear technology).[87] Other departments, including the Department of State and the Department of Defense, are involved in reviewing applications. Several bodies, including the NRC, the Department of Commerce, the Department of Homeland Security, the Department of Justice, and the federal courts are involved in enforcement.

The legal basis for these efforts is diverse and includes legislation, regulations promulgated by agencies such as the NRC, executive orders, and international agreements. In addition to being bound by treaties such as the CPPNM, the United States has, as a matter of policy, also undertaken to abide by various nonbinding international agreements, such as the Nuclear Suppliers Group guidelines, as well as codes of best practice, such as IAEA recommendations on nuclear security.

This description is far from exhaustive; it includes neither the oversight of military nuclear activities, which by definition are not dual-use, nor U.S. government activities to negotiate and implement international nonproliferation and nuclear security activities.

Rather than attempt to provide a more detailed description of the whole of the domestic oversight regime, this article focuses on two contested elements that highlight some of the fundamental challenges associated with managing dual-use

85. NRC, "International Safeguards."

86. The Department of Commerce also has a role in collecting information from private industry for the United States' additional protocol declarations.

87. Ian F. Fergusson and Paul K. Kerr, *The U.S. Export Control System and the President's Reform Initiative*, CRS Report for Congress, R41916 (Washington, D.C.: Congressional Research Service, January 13, 2014), 7, 26–27, https://www.fas.org/sgp/crs/natsec/R41916.pdf.

nuclear technologies: (1) the absence of a regularized procedure for assessing the nonproliferation consequences of domestic decisions; and (2) the nonproliferation and nuclear security conditions for international nuclear cooperation.

As exemplified by the licensing of GE Hitachi's laser enrichment plant, the United States has no formalized process for assessing the nonproliferation implications of domestic decisions to develop or use new nuclear technologies. A nonproliferation assessment *is* required when the United States concludes an agreement with another country to permit the transfer of nuclear material or equipment. As such, one was conducted when the United States and Australia reached an agreement (which was considered an addendum to their existing nuclear cooperation agreement) to transfer Silex technology from Australia to the United States. However, this assessment focused purely on the nonproliferation implications of the transfer and not on the implications of commercialization.

The NRC does not license fuel-cycle technologies per se. Rather, it licenses facilities, and the only nonproliferation implication it considers in doing so is the applicant's ability to protect classified information. However, the commission appears to have the necessary authority to require a much broader assessment. In March 2012, the Congressional Research Service concluded that, given the NRC's statutory responsibility to promote the "common defense and security," it "could reasonably conclude that it has sufficient existing authority to promulgate a regulation requiring that applicants provide the Commission with a proliferation risk assessment as part of the license application process."[88] A petition to require such an assessment for all new enrichment or reprocessing facilities was submitted by the American Physical Society but rejected by the NRC in June 2013. The NRC did not deny that new technologies might pose a proliferation risk but argued that Congress or the president was responsible for considering them.[89]

As a result of this decision, every part of the U.S. government has now eschewed responsibility for assessing the nonproliferation implications of domestic projects to develop new nuclear technologies or construct new facilities. Historically, the U.S. government has been more sensitive to the international implications of such decisions—although it has generally done so only where public funding was involved (which was not the case with GE Hitachi's laser enrichment plant). Most notable, nonproliferation was the main factor behind the U.S. moratorium on reprocessing (although contrary to what is often asserted, particularly by proponents of reprocessing, the Ford administration's initial decision was also a reflection of the need for the U.S. government

88. Todd Garvey, memorandum to Jeff Fortenberry, "Authority of the Nuclear Regulatory Commission to Require a Proliferation Risk Assessment as Part of a Uranium Enrichment Facility License Application," Congressional Research Service, March 27, 2012, 4, http://www.princeton.edu/~rskemp/CRS-opinion-on-NRC-authority.pdf.

89. R. W. Borchardt, "Denial of Petition for Rulemaking (PRM-70-9)—American Physical Society," SECY-12-0145, Nuclear Regulatory Commission, October 25, 2012, 4, 20, http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2012/2012-0145scy.pdf.

to subsidize the project).[90] The George W. Bush administration drafted but did not finalize a nonproliferation impact assessment for its Global Nuclear Energy Partnership program (which envisaged domestic reprocessing in the United States and potentially also in a small number of other states that already had access to the technology).[91] Even the NRC has historically assigned a bigger nonproliferation role to itself; for example, in 1976 it postponed the licensing of fuel exports to a U.S.-supplied nuclear reactor in India, following that state's 1974 nuclear test.[92] The export of fuel to India was not a purely domestic action (like building an enrichment or reprocessing facility), but it does demonstrate that the NRC has interpreted its mandate more broadly in the past than it does now. Ultimately, however, all of these initiatives were ad hoc. Only when key actors have had an interest in nonproliferation—or were forced to take one—has it been factored into domestic decisions.

The U.S. export control system, as Congressional Research Service analysts Ian Fergusson and Paul Kerr note, has "long been criticized by exporters, nonproliferation advocates, allies, and other stakeholders as being too rigorous, insufficiently rigorous, cumbersome, obsolete, inefficient, or any combination of these descriptions."[93] The 1954 Atomic Energy Act, as amended by the 1978 Nuclear Nonproliferation Act, provides two separate legal bases for international nuclear cooperation. Pursuant to section 123 of the act, "significant nuclear exports" (transfers of nuclear material, reactors, or certain reactor components) require an intergovernmental agreement, generally known as a "123 agreement."[94] Even with such an agreement in place, each individual export of equipment or material still requires a separate license, which is issued by the NRC. Separately, section 57.b of the Atomic Energy Act empowers the secretary of energy to authorize "technology transfers and technical assistance," provided that they "will not be inimical" to U.S. interests.[95] The procedures for authorizing such transfers are set out in title 10 of the *Code of Federal Regulations*, part 810, and are generally known as "810 agreements." Finally, nuclear technology and commodities that are not covered by the Atomic Energy Act—such as equipment that has both nuclear and nonnuclear applications—may still

90. Michael J. Brenner, *Nuclear Power and Non-proliferation: The Remaking of U.S. Policy* (Cambridge: Cambridge University Press, 1981), 100–113.

91. U.S. Department of Energy, National Nuclear Security Administration, Office of Nonproliferation and International Security, *Draft Nonproliferation Impact Assessment for the Global Nuclear Energy Partnership Programmatic Alternatives* (Washington, D.C.: National Nuclear Security Administration, December 2008), http://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/GNEP_NPIA.pdf.

92. Brenner, *Nuclear Power and Non-proliferation*, 84–88.

93. Fergusson and Kerr, *U.S. Export Control System and the President's Reform Initiative*, 1.

94. This phrase and its definition, which is an interpretation of the act, is from "123 Agreements," Export.gov, December 3, 2010, https://build.export.gov/main/civilnuclear/eg_main_022093.

95. This phrase, which is an interpretation of the act, is from "810 Authorization," Export.gov, February 9, 2011, https://build.export.gov/main/civilnuclear/eg_main_022094.

be controlled through the 1979 Export Administration Act.[96] This act requires Department of Commerce authorization for the transfer of technologies and items that appear on the Commerce Control List (which includes but is much broader than dual-use nuclear technology).

Although a high-profile effort to simplify the U.S. export control system is currently underway, it will not affect nuclear exports conducted pursuant to either 123 or 810 agreements.[97] Instead, the Obama administration has undertaken a separate effort to revamp 810 agreements while trying to head off congressional efforts designed to make 123 agreements more restrictive.

The existing regulations for 810 agreements define a set of "generally authorized" activities that have received prior approval from the secretary of energy and can therefore be conducted abroad without "specific authorization." However, the regulations also contain a list of states for which this exemption does *not* apply and for which specific authorization is required on an activity-by-activity basis. With the most significant of its proposed changes, the Obama administration seeks to reverse this approach by specifying those states for which general authorization *does* apply. The Nuclear Energy Institute, which lobbies on behalf of the nuclear industry, has opposed this approach on various grounds, including that it would increase, by seventy-seven, the number of states requiring specific authorization.[98] In response, the Obama administration has argued that the number of transfers to these states is so small that the security benefits of the change would outweigh the costs.

Efforts to revise the requirements for 123 agreements have been more controversial. In 2009, the United States and the United Arab Emirates concluded a nuclear cooperation agreement under which the latter made a legally binding commitment not to acquire enrichment or reprocessing technology. Inevitably, this agreement raised the question of whether the United States would require other states to make a similar promise—termed the "gold standard" by the Obama administration (though it subsequently walked away from this term). Following a prolonged series of internal reviews, which were eventually concluded in late 2013, the administration announced a policy of deciding on a "case-by-case" approach whether to insist upon the would-be partner's renouncing enrichment and reprocessing.[99] Since then the administration has concluded an agreement with Taiwan, which did make a binding undertaking not to acquire enrichment or reprocessing technology, and one with Vietnam,

96. This act is currently expired but enforced through a presidential declaration of a national emergency. Fergusson and Kerr, *U.S. Export Control System and the President's Reform Initiative*, 2–3.

97. Ibid., 11.

98. For a discussion of the nuclear industry's objections and the administration's responses, see Mark Hibbs, "New and Balanced Rules for U.S. Nuclear Technology Exports," Carnegie Endowment for International Peace, September 30, 2013, http://carnegieendowment.org/2013/09/30/new-and-balanced-rules-for-u.s.-nuclear-technology-exports/hf9f.

99. Daniel Horner, "U.S. Policy on Nuclear Pacts Detailed," *Arms Control Today* 44 (January/February 2014), http://legacy.armscontrol.org/act/2014_01-02/US-Policy-on-Nuclear-Pacts-Detailed.

which did not—although Hanoi did express its intent, in nonbinding language, "to rely on existing international markets for nuclear fuel services, rather than acquiring sensitive nuclear technologies."[100]

An effort to try to force the administration into incorporating the "gold standard" into future 123 agreements has, however, gained some traction in Congress. Legislation has been introduced that would add a legally binding commitment not to acquire enrichment or reprocessing technology to the list of requirements that qualifies a 123 agreement for expedited review.[101] An eligible agreement enters into force ninety days of "continuous session" after it has been presented to Congress, unless legislative action is taken to block it. By contrast, an agreement that does not meet all the requirements must secure congressional approval before it becomes operative. The effect of the proposed legislation would, therefore, be to make it extremely difficult for a 123 agreement to enter into force unless the partner foreswore enrichment and reprocessing.

The fundamental debate here is (or, perhaps, ought to be) over the value of a nuclear cooperation agreement with the United States at a time when states that want to acquire nuclear power reactors can choose from a growing list of vendors. For much of the Cold War, the United States and the Soviet Union were essentially the only two suppliers of nuclear reactors—meaning that many states effectively had no choice. Today, there are commercial suppliers from seven states, and there is little reason to suppose this number will not grow slowly over time.[102] The Obama administration has argued (fairly persuasively in my opinion) that if it were to demand that potential buyers renounce enrichment and reprocessing they would simply go elsewhere, resulting in a loss for both U.S. industry *and* nonproliferation, since other supplier states impose less-rigorous nonproliferation requirements than the United States.[103] Proponents of the "gold standard" do not tend to refute this argument directly so much as urge the United States not to be complicit in aiding states to develop nuclear power programs that could, in the future, be used to advance military

100. Quoted in Daniel Horner, "Vietnam Nuclear Pact Sent to Congress," *Arms Control Today* 44 (June 2014), http://legacy.armscontrol.org/act/2014_06/News_Briefs/Vietnam-Nuclear-Pact-Sent-to-Congress.

101. For a more comprehensive summary of the most recent legislation, see Paul K. Kerr and Mary Beth D. Nikitin, *Nuclear Cooperation with Other Countries: A Primer*, CRS Report for Congress, RS22937 (Washington, D.C.: Congressional Research Service, December 3, 2015), 9, https://www.fas.org/sgp/crs/nuke/RS22937.pdf.

102. One complication here is that a number of non-U.S. reactor designs use U.S. technology and so can only be purchased by a buyer with a 123 agreement in force. Exactly which reactors fall into this category is unclear, but the list is likely to shrink over time.

103. Thomas M. Countryman, *Testimony of Assistant Secretary Thomas M. Countryman on Administration Policy Related to Agreements for Peaceful Nuclear Cooperation (123 Agreements)*, January 30, 2014, 3–4, http://www.foreign.senate.gov/imo/media/doc/Countryman_Testimony2.pdf.

goals. This debate is not unique to nuclear technology; the possibility that raising the requirements for exports could be counterproductive if not all suppliers agree to do so is a dilemma in any form of sensitive technology trade where multiple potential sellers are in competition with one another.

CURRENT STATE OF DOMESTIC OVERSIGHT IN OTHER COUNTRIES

Nuclear Nonproliferation Oversight

Five nuclear-weapon states are recognized by the NPT. Like the United States, each has a "voluntary offer" arrangement with the IAEA and has an additional protocol in force—although the scope of these agreements is highly variable.[104] In practice, the IAEA chooses to safeguard few of the eligible facilities. Most of the facilities that are safeguarded were selected because they use foreign technology or process foreign material, and the application of safeguards was a condition of supply. For example, a Russian-supplied centrifuge enrichment plant in China is under safeguards.

Four nuclear-armed states are not party to the NPT: India, Israel, Pakistan, and North Korea.[105] Israel and Pakistan never joined the treaty but agreed to IAEA safeguards on a few foreign-supplied facilities as a condition of supply. India also did not join the treaty but, pursuant to the U.S.-India nuclear deal, agreed to separate its military and civilian nuclear sectors and safeguard the whole of the latter (which includes domestically manufactured power reactors).[106] North Korea withdrew from the NPT in 2003 and currently does not allow any IAEA safeguards, including on foreign-supplied facilities.

The biggest category of states that are party to the NPT consists of those that do not possess nuclear weapons and are required to accept IAEA safeguards on all of their nuclear activities. The extent of these safeguards depends on whether the state has accepted an additional protocol and whether the amount of nuclear material it possesses is so small that it qualifies for a so-called small quantities protocol (which holds most of the requirements of a comprehensive safeguards agreement in abeyance to reduce the burden on the state).

In non-nuclear-weapon states, the primary nonproliferation role of domestic regulatory agencies is to cooperate with the IAEA to allow the implementa-

104. IPFM, *Global Fissile Material Report 2007*, 67–81.

105. South Sudan, which was founded only in 2011 and is not known to conduct any nuclear activities, has also not acceded to the treaty but is expected to do so in the not-too-distant future.

106. Problematically, the decision about which facilities were civilian and which were military was an exclusively Indian one. For a critique of the plan, see Zia Mian, A. H. Nayyar, R. Rajaraman, and M. V. Ramana, *Fissile Materials in South Asia: The Implications of the U.S.-India Nuclear Deal*, Research Report no. 1 (Princeton, NJ: IPFM, September 2006), 16–24, http://fissilematerials.org/library/rr01.pdf.

tion of safeguards. All non-nuclear-weapon states are required to have a "state system of accounting and control" to track nuclear materials and provide data to the IAEA (though such a system can also play an important role in nuclear security by detecting any unauthorized removal of nuclear material). These systems vary in effectiveness. For example, in 2004, the Egyptian Atomic Energy Authority (which operates that country's system of accounting and control) was reportedly forced to inform the IAEA that "it did not have the authority necessary for it to exercise effective control of all nuclear material and activities in the State."[107] Less dramatic problems with safeguards implementation are routine. For example, a leaked IAEA document reveals that, in 2012, seventy-one states, most of which are developing, routinely missed reporting deadlines. A few more-developed states operating research or power reactors, including Brazil, China, Mexico, and Poland, sometimes did so too.[108]

In many non-nuclear-weapon states, constitutional provisions, laws, or fatwas forbid the development of nuclear weapons. While these may play a role in nonproliferation—by encouraging whistle-blowing or empowering domestic opponents of nuclear-weapon development, for example—there is an obvious tension in self-regulation; that is, in a government overseeing the implementation of its own nonproliferation commitments. For this reason, domestic nonproliferation oversight of dual-use nuclear activities is very much secondary to international oversight.

In theory, domestic processes could play an important role in helping states to consider the international implications of domestic nuclear energy decisions. To the best of this author's knowledge, however, no state currently has a formalized process for factoring proliferation implications into domestic licensing decisions—although, like the United States, some states have occasionally created one-off processes. In the United Kingdom, for example, a judicial inquiry was held in 1977 into a hugely controversial plan to construct a new reprocessing plant. Proliferation was extensively discussed during this inquiry—although the presiding judge reached the somewhat unexpected conclusion that the construction of THORP, as the facility was called, would advance nonproliferation ends since foreign states would be able to separate plutonium in the United Kingdom and so would not need to construct their own facilities.[109] (For the record, the United Kingdom's most important foreign client, Japan, did eventually build its own domestic facility anyway, which should have surprised no one since that was Tokyo's stated long-term policy at the time of the inquiry.)

107. Pierre Goldschmidt, "The IAEA Reports on Egypt: Reluctantly?" Carnegie Endowment for International Peace, June 2, 2009, http://carnegieendowment.org/2009/06/02/iaea-reports-on-egypt-reluctantly/1ztv.

108. Mark Hibbs, "Safeguards in the Spotlight," *Arms Control Wonk* (blog), June 9, 2013, http://hibbs.armscontrolwonk.com/archive/1878/safeguards-in-the-spotlight.

109. For a trenchant critique of the process, see William Walker, *Nuclear Entrapment: THORP and the Politics of Commitment* (London: Institute for Public Policy Research, 1999), 13–27.

If nothing else, this experience demonstrates just how difficult and controversial proliferation assessments can be.

Domestic processes play a more important role in export controls. The two international nuclear export control arrangements—the Zangger Committee and the Nuclear Suppliers Group—seek to harmonize standards. However, their effectiveness in this regard is limited, both because they are not universal and because their guidelines are designed to permit some significant differences in procedures and policy between participating governments.[110] For example, the complexity of the U.S. export control system—its three-way split of responsibility for regulating nonmilitary exports, in particular—appears to be unparalleled. By contrast, in some states, including Japan and Russia, all nuclear-related exports are licensed by a single agency.

Differences in policy are more interesting. The United States requires other states to seek prior consent before reprocessing U.S.-origin spent fuel (which includes any fuel that has "passed through" U.S. technology, including in fuel fabrication facilities and reactors). Japan has followed this model in all of its nuclear cooperation agreements with non-nuclear-weapon states except Kazakhstan. By contrast, France, Russia, and South Korea have not included such a provision in their nuclear cooperation agreements (with the exception of the South Korea–UAE agreement).[111] These states' policies toward retransfers also differ (in practice, the only item involved in nuclear power generation that could conceivably be retransferred is spent fuel sent for reprocessing or storage abroad).[112] France, Japan, South Korea, and the United States generally require importers to seek their permission before reexporting controlled items. Russia, however, generally demands only that the retransfer has the same conditions attached as the original transfer (although it does require prior consent for the retransfer of particularly sensitive items, such as separated plutonium or HEU).

Although the United States generally does insist on more demanding conditions for nuclear cooperation than do other states, there are exceptions—as highlighted, for example, by nuclear cooperation with India. All major nuclear exporters have now concluded cooperation agreements with New Delhi except for Tokyo, which is seeking a unique provision allowing it to terminate cooper-

110. The differences highlighted in the following paragraphs are drawn from James A. Glasgow, Elina Teplinsky, and Stephen L. Markus, *Nuclear Export Controls: A Comparative Analysis of National Regimes for the Control of Nuclear Materials, Components and Technology* (Washington, D.C.: Pillsbury Winthrop Shaw Pittman LLP, October 2012), http://www.pillsburylaw.com/siteFiles/Publications/NuclearExportControls.pdf. This study was commissioned by the Nuclear Energy Institute, a lobbying organization for the nuclear industry, to highlight ways in which U.S. export controls are more burdensome than the export controls of American competitors. Although no evidence is presented to substantiate its assertions about potential buyers' concerns about the U.S. export control system, its purely factual analysis of the differences between states appears to be reliable and carefully researched.

111. Ibid., 51.

112. Ibid.

ation should India conduct another nuclear test, as well as verification requirements that go beyond IAEA safeguards.[113]

Controlling exports of equipment with both nuclear and nonnuclear uses is, however, probably more challenging than regulating exports of reactor fuel and components, both because the former are much more difficult to track and because far more states are involved in their production and transshipment. The A. Q. Kahn network, for example, manufactured many centrifuge components in Malaysia and used the United Arab Emirates as a key transshipment node. Neither state was—or is—a participant in the Nuclear Suppliers Group. At the time, the absence of any meaningful export controls was the norm for such states (even for states within the Nuclear Suppliers Group, export controls often left a lot to be desired).

Reporting pursuant to UNSCR 1540, which mandates the creation and enforcement of export controls, gives some sense of the current state of play. A survey of thirty-eight states' reports from 2008 revealed large disparities in implementation, with less-developed states having generally instituted fewer of the resolution's requirements.[114] The most neglected requirements related to so-called deemed exports (in-country transfers of intangible commodities to foreign nationals) and controls over both proliferation financing and transportation services.[115] In these areas, 16–42 percent of the states surveyed had legislation in force that provided for some type of control. Moreover, enforcement lagged behind the creation of a legal framework in most of the areas in which the resolution requires states to act.

Nuclear Security

Domestic nuclear security is similar to export controls in that national requirements and the quality of implementation vary widely (even if all states can agree on the goal of preventing unauthorized access to nuclear materials and facilities). By far the most comprehensive survey of nuclear security standards is the Nuclear Threat Initiative's *Nuclear Materials Security Index*.[116] This index scores states on nineteen indicators grouped in five categories. Two of these categories—"quantities and sites" (comprising indicators such as the quantity of nuclear material in a state, how many sites the material is stored at, and how frequently it is transported) and "risk environment" (comprising indicators such as political stability and the pervasiveness of corruption)—are made up of fac-

113. Dipanjan Roy Chaudhury, "Prime Minister Narendra Modi's Japan Visit May Not Seal Civil Nuclear Deal," *Economic Times*, August 30, 2014, http://articles.economictimes.indiatimes.com/2014-08-30/news/53387773_1_india-and-japan-india-japan-japan-visit.

114. Peter Crail, "Measuring Nuclear Export Controls in Nuclear-Powered Nations and Nuclear Aspirants," in *A Collection of Papers from the 2010 Nuclear Scholars Initiative*, ed. Mark Jansson (Washington, D.C.: Center for Strategic and International Studies, 2010), 80–87, available from http://csis.org/publication/collection-papers-2010-nuclear-scholars-initiative.

115. U.S. Department of Commerce, Bureau of Industry and Security, "Deemed Exports," n.d., https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.

116. Nuclear Threat Initiative, *NTI Nuclear Materials Security Index*.

tors that a regulator cannot reasonably be expected to affect. The remaining three categories, comprising twelve indicators, rate a state's legal infrastructure and the general nuclear security requirements it imposes, its involvement in international agreements and initiatives, and the extent to which international undertakings have actually been enshrined in domestic legislation. The index does not examine the specifics of security arrangements at individual sites, which generally are (and indeed should be) secret. That said, in a number of states, even information about general nuclear security requirements is not available.

To help identify, in a crude sense, where states' nuclear security standards differ most from one another, the following list shows the twelve indicators of regulatory effectiveness in order of decreasing variance among states (i.e., states' scores are most widely spread in item 1 and least widely spread in item 12; only scores from the twenty-five states with at least one kilogram of weapon-usable nuclear material are included).[117]

1. Physical security during transport
2. Independent regulatory agency
3. Control and accounting procedures
4. Domestic nuclear materials security legislation
5. International assurances
6. International legal commitments
7. Voluntary commitments
8. UNSCR 1540 implementation
9. Safeguards adherence and compliance
10. Insider threat prevention
11. On-site physical protection
12. Response capabilities

The biggest differences among the twenty-five states lie in their standards for physical security during transport, whether they have an independent regulator, and in their control and accounting procedures. Ten states (including the United States) have regulations consistent with the IAEA's most recent nuclear security guidance, INFCIRC/225/rev.5; ten (including China, Japan, and Russia) have guidance consistent with a slightly older version, INFCIRC/225/rev.4, which places less of an emphasis on testing security systems, including with "force-on-force" exercises; and five (Argentina, India, Pakistan, South Africa, and Uzbekistan) have still lower or no published standards. Separately, the states' scores on the regulatory independence indicator are widely spread because three of the twenty-five (India, Iran, and North Korea) lack an indepen-

117. Author's calculations based on data from Nuclear Threat Initiative, *NTI Nuclear Materials Security Index*.

dent regulator.[118] Finally, states' scores for control and accounting procedures differ widely, principally because of varying rules for access controls (requiring identity checks for people entering sensitive areas and keeping appropriate records). Overall, the *Nuclear Materials Security Index* contains some surprises about which states perform well and poorly. Belarus, for example, achieves perfect scores for its physical security standards, the independence of its regulator, and its control and accounting procedures. By contrast, Belgium's requirements for physical protection during transport and access controls fall short of internationally recognized best practice.

One problem with the *Nuclear Materials Security Index* is that it does not consider enforcement. Russia and the United States (along with Kazakhstan) are the top-ranked nations for preventing insider threats. However, even if Russian regulations are consistent with best practice, evidence suggests that implementation has been lacking.[119] For example, Matt Bunn, a former U.S. government official, recalls visiting a Russian nuclear facility in the mid-2000s and seeing two portal monitors to detect radiation, one American and one Russian. When he asked why there were two monitors, he was told that the U.S. monitor was deactivated on Thursdays, when plant activities tended to set it off accidentally, and the less sensitive Russian monitor was used instead.[120] He notes that because "every insider was aware of this practice, and would know to plan an attempted theft for a Thursday," this procedure rendered the U.S. system "largely pointless."

Another example of an implementation challenge concerns assessments of the security threats that facilities are designed to withstand. Best practice requires the development of—and regular updates to—so-called design basis threats. Not only does the *Nuclear Materials Security Index* not give Japan credit in this category, apparently because Japanese regulations impose no requirement for regular updates, but most, if not all, Japanese facilities are not designed to withstand attack by armed terrorists.[121] U.S. visitors to Japanese nuclear facilities are generally surprised by the lack of armed guards (which is in part a consequence of legal restrictions on the use of guns by private security firms). While Japanese officials have insisted, with some justification, that armed terrorism is unlikely in Japan, the fact that the country has been the victim of

118. Although only three states lack an independent regulator, the spread of scores is large because this indicator is a binary variable. Whether this should be considered a bug or a feature of this approach is up for debate.

119. Togzhan Kassenova, *From Antagonism to Partnership: The Uneasy Path of the U.S.-Russian Cooperative Threat Reduction* (Stuttgart: ibidem Press, 2007), 178, 189, 209; and Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge, Mass.: American Academy of Arts and Sciences, 2014), 9, 11, 14, https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf.

120. Bunn and Sagan, *A Worst Practices Guide to Insider Threats*, 11.

121. Douglas Birch, R. Jeffrey Smith, and Jake Adelstein, "Japan Could Be Building an Irresistible Terrorist Target, Experts Say," Center for Public Integrity, March 11, 2014, http://www.publicintegrity.org/2014/03/11/14366/japan-could-be-building-irresistible-terrorist-target-experts-say.

chemical attacks by an apocalyptic cult suggests that armed attacks on nuclear facilities should not be considered impossible. To be fair, Japan's nuclear security system does seem to be improving, and armed police are now present at its most sensitive facility, the Rokkasho Reprocessing Plant—but progress appears to be slow. The Japanese experience also raises the question of the extent to which nuclear security measures can safely be adapted to local cultural norms and laws (such as restrictions on private gun ownership).

OTHER MODELS FOR MANAGING THE RISK FROM NUCLEAR TECHNOLOGY

Today any ambition to reform the nuclear nonproliferation regime is markedly lacking. Almost all governmental and nongovernmental efforts to bolster the regime as a whole (as opposed to those focused on country-specific challenges, most notably from Iran) aim to achieve incremental change.[122] In some part at least, this emphasis on gradual evolution is the result of the failure, last decade, of two ambitious—perhaps revolutionary—"big ideas."

In 2004, George W. Bush identified what he termed a "loophole" in the NPT that allows states "to produce nuclear material that can be used to build bombs under the cover of civilian nuclear programs."[123] In response, he called upon "the world's leading nuclear exporters" to provide reliable nuclear fuel supplies to states that renounced enrichment and reprocessing, and he called upon the Nuclear Suppliers Group to ban the transfer of these technologies to states that did not already possess them.

These proposals met with considerable opposition from such states, including close U.S. allies such as Australia and Canada. Some states that did have the technology opposed them too. In the event, the Nuclear Suppliers Group took more than seven years to agree on a relatively permissive and distinctly ambiguous set of criteria under which exports of enrichment and reprocessing facilities would be permitted.[124] Today, the Nuclear Suppliers Group's participating governments show little appetite to reopen the debate.

Bush's call for reliable fuel assurances also contributed to a debate, started by then IAEA Director General Mohamed ElBaradei the previous year, about the internationalization or multilateralization of the nuclear fuel cycle. The idea of taking sensitive nuclear activities out of the hands of individual states has been periodically revisited since it was first proposed in the Acheson-Lilienthal

122. The one possible exception is Obama's renewed focus on nuclear disarmament. However, this initiative seeks to enhance the nonproliferation regime indirectly, by using disarmament to motivate a coalition willing to strengthen nonproliferation rules. Besides, it has now been largely abandoned by the White House.

123. George W. Bush, remarks, Washington, D.C., February 11, 2004, http://2001-2009.state.gov/t/isn/rls/rm/29290.htm.

124. For a critique of the new rules, see Hibbs, "New Global Rules for Sensitive Nuclear Trade."

report, which suggested that all such activities be conducted by an international organization. Moreover, multilateral (but not truly international) coalitions have been set up for enrichment, including Urenco, which was created by the British, Dutch, and German governments to develop and operate centrifuge technology, and Eurodif, under which France, Belgium, Italy, and Spain (and, at various times, Sweden and Iran) owned a gaseous diffusion plant in France that has recently been shut down.[125]

ElBaradei reawakened this debate in 2003 when he proposed that enrichment and reprocessing should take place only in "facilities under multinational control."[126] This suggestion, combined with Bush's call for reliable fuel assurances, sparked a plethora of proposals from governments and nongovernmental organizations.[127] Some of the proposals merely sought to reinforce existing market mechanisms. Others were extremely ambitious and involved complex international ventures. The German contribution, for example, proposed that the IAEA should own a new enrichment facility in an extraterritorial area (i.e., an area outside the control of any nation-state). Most of these proposals did not incorporate Bush's suggestion that fuel supply assurances be extended only to governments that renounced enrichment and reprocessing (even the U.S. government eventually dropped this requirement from its proposals). Nonetheless, because of their complexity and, more important, a lack of interest from governments, all of the more-ambitious proposals quickly fell by the wayside—and seem unlikely to be revived in the short term. Three modest initiatives did make it off the ground. However, the only one that can be described as multinational is the International Uranium Enrichment Center, a Russian venture owned jointly with Armenia, Kazakhstan, and Ukraine that has access to some of the output from a Russian centrifuge facility.[128]

Domestic nuclear nonproliferation policy is, in theory at least, more susceptible to faster change since the buy-in of only one state is required. States could, for example, require themselves to conduct an assessment of the non-

125. The centrifuge technology Urenco developed is now owned by the Enrichment Technology Corporation, which since 2006 has been jointly owned by the British, Dutch, and German governments and France's Areva.

126. Mohamed ElBaradei, "Towards a Safer World," *Economist*, October 16, 2003, http://www.economist.com/node/2137602.

127. For a summary of some of these proposals, see Mary Beth Nikitin, Anthony Andrews, and Mark Holt, *Managing the Nuclear Fuel Cycle: Policy Implications of Expanding Global Access to Nuclear Power*, CRS Report for Congress, RL34234 (Washington, D.C.: Congressional Research Service, October 19, 2012), https://www.fas.org/sgp/crs/nuke/RL34234.pdf; and Yury Yudin, *Multilateralization of the Nuclear Fuel Cycle: Assessing the Existing Proposals* (Geneva: United Nations Institute for Disarmament Research, 2009), http://www.unidir.org/files/publications/pdfs/multilateralization-of-the-nuclear-fuel-cycle-assessing-the-existing-proposals-345.pdf.

128. The other initiatives that are being or have been implemented are "fuel banks" (actually uranium hexafluoride banks) to cater to states that suffer a politically motivated disruption of fuel supply. One has been set up by Russia, which pays for and operates this facility, but the responsibility for releasing material lies with the IAEA. Second, the IAEA has approved and is in the process of establishing a similar facility in Kazakhstan. Much of the funding for this facility came from the Nuclear Threat Initiative and the U.S. government.

proliferation implications of domestic licensing decisions. Yet the effort in the United States to petition the NRC to do just that has failed, and no discussion of the idea appears to be ongoing elsewhere. That said, another aspect of nuclear regulation—safety—does provide a clear precedent for such an assessment. Specifically, a basic principle of radiation safety is that "facilities and activities that give rise to radiation risks must yield an overall benefit."[129] This principle has led to a formal requirement for all European Union states to "ensure that all new classes or types of practice resulting in exposure to ionizing radiation are justified in advance of being first adopted or first approved by their economic, social or other benefits in relation to the health detriment they may cause."[130] If the word *health* is changed to *proliferation*, this requirement nicely captures the goal of a nonproliferation assessment.

In contrast to nuclear nonproliferation, one big idea *is* under discussion for nuclear security: the creation of a universal, comprehensive, legally binding nuclear security regime that requires states to take steps to demonstrate their compliance. Several variations on this central theme have been proposed. One idea is to develop a framework agreement for nuclear security—similar to, say, the UN Framework Convention on Climate Change—that would set out basic nuclear security principles and "allow for the negotiation of supplementary protocols that require more detailed nuclear security actions."[131] Another idea is for states to agree to give the IAEA (or another international body) "the authority to define, review, and monitor national nuclear security standards and to evaluate compliance."[132] These ideas have, so far at least, largely been championed by nongovernmental experts seeking to ensure that the momentum generated by the Nuclear Security Summit process is not lost after the 2016 meeting, which is expected to be the last. So far, none of the states participating in the process have endorsed the idea of a comprehensive and legally binding nuclear security treaty because they worry it would be too bureaucratic, unwieldy, and difficult to negotiate. That said, their initially negative reactions do appear to have softened somewhat.

129. IAEA, *Fundamental Safety Principles*, Safety Fundamentals SF-1 (Vienna: IAEA, 2006), 10, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf.

130. European Council Directive 96/29/EURATOM, May 13, 1996, title IV, chap. I, art. 6, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01996L0029-20000513&from=EN.

131. NSGEG, *Responsibility beyond Rules*, 14.

132. Boureston and Ogilvie-White, "Seeking Nuclear Security through Greater International Coordination," 11.

OVERSIGHT CHALLENGES: STRUCTURAL BARRIERS TO CHANGE

Given the relatively limited role of individual scientists, the key actors in both domestic and international debates over the regulation of dual-use nuclear technology are governments and the nuclear industry—which are often one and the same. Two main fault lines traverse the international politics of nuclear regulation: between the states that possess nuclear weapons and those that do not; and between the states that possess nuclear technology and those that do not. Although the nuclear-armed states largely overlap the technology holders, the two groups are not identical. Germany, Japan, and the Netherlands, for example, all possess sensitive nuclear technology but do not have nuclear weapons. And the two fault-lines, although not perfectly predictive of states' positions—Western European countries without nuclear weapons, for example, tend to side with the nuclear-weapon states on a number of issues—are probably the most important determinant.

States without a particular type of nuclear technology—whether nuclear reactors, enrichment, or reprocessing—are often concerned about protecting, both legally and practically, their ability to acquire that technology in the future, even if they have no plans to do so. The United Arab Emirates and Taiwan are, for example, likely to prove fairly unusual in being willing to renounce enrichment and reprocessing. Vietnam's position—to insist on preserving what it sees as a right, even though it appears to have little interest in exercising it—is much more common. The Nuclear Suppliers Group guidelines on the transfer of enrichment and reprocessing technology took so long to negotiate because a number of states without such technology, including Canada, South Korea, and Turkey, wanted to keep open the option of acquiring it.[133] Their position was even shared by some states with enrichment facilities, including Brazil and Argentina, which appear to have been taking a "principled" stance against technology denial, as well as protecting their ability to acquire new forms of enrichment and reprocessing technology in the future. One example of how deep concern about technology denial among some of these state runs is that when Brazil and Turkey negotiated a (never implemented) fuel swap with Iran in 2010, to try to help diffuse the crisis, they stated in their joint declaration that "Turkey and Brazil appreciated Iran's . . . constructive role in pursuing the realization of nuclear rights of [the NPT's] Member States."[134]

Even proposals that do not explicitly involve restrictions on technology are often treated with skepticism by the "have-nots" out of concern for a hidden agenda. The clumsy rollout of U.S. nonproliferation proposals in 2004, when Bush *did* explicitly condition U.S. fuel supply assurances on states' renouncing enrichment and reprocessing technology, did a lot to feed this fear—and it has persisted long after Washington ceased to talk about technology denial.

133. McGoldrick et al., *Limiting Transfers of Enrichment and Reprocessing Technology*, 13–17.

134. Manucher Mottaki, Ahmet Davutoğlu, and Celso Amorim, *Joint Declaration by Iran, Turkey and Brazil*, May 17, 2010, para. 10, https://fas.org/nuke/guide/iran/joint-decl.pdf.

Discussions about multilateralizing or internationalizing the fuel cycle during the late 2000s were, for example, made much more difficult by "the common misconception that any multilateral mechanism necessarily implies the deprivation of the [NPT] Article IV right of [non-nuclear-weapon states] to peaceful nuclear technology."[135] Fear of technology denial affected progress in nuclear security too. In 2009, for example, the U.S. and UK governments pushed the idea of making nuclear security a fourth "pillar" of the NPT to stand alongside the existing three of nonproliferation, disarmament, and the peaceful use of nuclear energy. Many states, particularly within the Non-Aligned Movement, viewed this as an attempt to create additional obligations that would interfere with their "inalienable right" to use nuclear energy.[136] The British and American governments rapidly dropped the idea. If the United States and other like-minded governments were to back the idea of a comprehensive and legally binding nuclear security treaty, many states might interpret it as another attempt at technology denial. Disagreements over the severity of the threat from nuclear terrorism would serve only to exacerbate their suspicion.

Discussions about strengthening nonproliferation and nuclear security also bring out the tensions between nuclear-weapon states and non-nuclear-weapon states over disarmament. Although non-nuclear-weapon states have expressed dissatisfaction that the Obama administration's push on nuclear security has come at the expense of disarmament, the issue of nonproliferation is where the acrimony really comes to the fore.[137] Almost any proposal to strengthen the nonproliferation regime is opposed by many non-nuclear-weapon states, especially within the Non-Aligned Movement, on the grounds that the nuclear-weapon states have failed to live up to their disarmament commitments (which, among non-nuclear-weapon states, increasingly seems to mean negotiating a time-bound treaty to abolish nuclear weapons).

Whether the lack of progress on disarmament is a genuine reason or a convenient excuse for those non-nuclear-weapon states that oppose strengthening the nonproliferation regime has been the subject of much debate.[138] This author has come to the conclusion that many non-nuclear-weapon states do feel genuine frustration at what they see as the nuclear-weapon states' failure to live up to the disarmament bargain, and do seek to leverage nonproliferation to

135. Yury Yudin, *Multilateralization of the Nuclear Fuel Cycle: The Need to Build Trust* (Geneva: United Nations Institute for Disarmament Research, 2010), 10–11, http://www.unidir.org/files/publications/pdfs/multilateralization-of-the-nuclear-fuel-cycle-the-need-to-build-trust-132.pdf.

136. Bowen, Cottee, and Hobbs, "Multilateral Cooperation and the Prevention of Nuclear Terrorism," 357. The phrase "inalienable right" is from article IV of the NPT.

137. Deepti Choubey, *Are New Nuclear Bargains Attainable?* (Washington, D.C.: Carnegie Endowment for International Peace, 2008), http://carnegieendowment.org/files/new_nuclear_bargains.pdf.

138. Although slightly dated, a trenchant discussion with a useful agenda for moving forward is Christopher F. Chyba, "Time for a Systematic Analysis: U.S. Nuclear Weapons and Nuclear Proliferation," *Arms Control Today* 38 (December 2008), http://www.armscontrol.org/act/2008_12/Chyba.

achieve their disarmament goals. However, rarely is disarmament the *only* reason why key non-nuclear-weapon states oppose any given nonproliferation measure. For example, Togzhan Kassenova, a scholar of Brazil's nuclear program, concludes that Brasilia's objections to the additional protocol are multifaceted and include, for example, a desire not to compromise sensitive information related to its nuclear submarine or centrifuge programs, as well as frustration over the pace of disarmament.[139] In public, however, it is much easier for Brazil to justify its position by simply blaming the nuclear-weapon states. Strengthening the nonproliferation regime is likely to prove difficult if many non-nuclear-weapon states' opposition is overdetermined in this way; specifically, progress toward disarmament may be a necessary condition, but it is unlikely to prove sufficient.

The nuclear industry also tries to influence nonproliferation and nuclear security policy. The industry can sometimes be a direct participant in debates, particularly domestic ones. At other times, it is an indirect participant, seeking to influence the position that its national government carries into international discussions. That said, because so much of the global nuclear industry is state-owned, it is probably more accurate not to think of the nuclear industry as an independent actor in many states but to characterize national debates over nuclear policy as bureaucratic processes, internal to government, in which nuclear industrial considerations are an important factor.

That said, the nuclear industry is really two separate industries: operators and vendors (particularly of nuclear reactors and reactor components). The former has a general and somewhat visceral predisposition to oppose additional regulation and generally tries to deny any link between nuclear power and proliferation. Moreover, operators sometimes object to additional nonproliferation or nuclear security measures on more concrete grounds. Brazil's centrifuge operators, for example, are opposed to the additional protocol. "Grumblings about the cost and perceived unfair safeguards burden" are often heard from diplomats representing states, including Canada, Germany, and Japan, that have large nuclear industries.[140] Despite their concerns, operators, for at least three reasons, are probably not a major barrier to improvements in nonproliferation and security. First, because so few nuclear facilities in the nuclear-weapon states are safeguarded, a major source of potential opposition is effectively nullified. Second, particularly where nuclear security is concerned, many operators recognize how damaging an incident could be to the health of the nuclear industry as a whole. Third, the cost of safeguards and nuclear security is relatively small (especially when compared to safety).

Vendors, by contrast, have a bigger influence on policy. Within the United States, reactor and component vendors, which are not state-owned, constitute

139. Togzhan Kassenova, *Brazil's Nuclear Kaleidoscope: An Evolving Identity* (Washington, D.C.: Carnegie Endowment for International Peace, 2014), 60–62, http://carnegieendowment.org/files/brazil_nuclear_kaleidoscope_lo_res.pdf.

140. Trevor Findlay, *Nuclear Energy and Global Governance: Ensuring Safety, Security and Non-proliferation* (Abingdon: Routledge, 2011), 145.

a powerful lobby that has opposed (on relatively solid grounds) congressional efforts to tighten the conditions under which 123 agreements can be concluded and (with much flimsier arguments) administration efforts to revamp the rules for 810 agreements. Meanwhile, although the policy-formation process is much more opaque, industrial considerations almost certainly play a major role in influencing the policies of the states that own major exporters, including France and Russia.

That does not mean raising revenue is the only purpose of reactor sales; they are also a tool of foreign policy. For example, the provision of a nuclear power plant, with generous financing arrangements, was integral to achieving a package of energy agreements that Russia struck with Turkey in 2010.[141] A government's desire for flexibility, so that nuclear power plant sales can be used to further other foreign policy goals, adds yet another layer of opposition to tightening rules for exports. A desire to facilitate "strategic" reactor sales can even lead governments to undermine those nuclear nonproliferation rules that are in place. The U.S.-India nuclear deal—under which the United States sought an exemption from Nuclear Suppliers Group rules to enable reactor sales to India—was, from the U.S. perspective at least, primarily motivated by the goal of forging a strategic partnership with India, particularly against China.[142] Similarly, furthering a strategic partnership appears to have been one important motivation behind China's decision to supply reactors to Pakistan. A cliché within the nuclear policy community is that nonproliferation goals almost always lose out when they conflict with efforts to strengthen a bilateral relationship.

***

"The exceptional nature of nuclear weapons," the political scientist William Walker wrote in 2007, "calls for an exceptional kind of cooperative politics."[143] The use of nuclear weapons represents the highest level of violence to which humanity can resort. Even a single weapon could lead to hundreds of thousands, or even millions, of deaths, appalling suffering of the survivors, the extensive destruction of property, and widespread radioactive contamination. To be sure, deterrence may continue to prevent use. However, deterrence is likely to become riskier as more states acquire nuclear weapons and to become particularly unreliable should nonstate actors do so. Moreover, states worry

141. For details of the package, see Sebnem Arsu, "Turkey's Pact with Russia Will Give It Nuclear Plant," *New York Times*, May 12, 2010, http://www.nytimes.com/2010/05/13/world/europe/13turkey.html. For the background, see Center for Strategic and International Studies, Economic Policy Research Foundation of Turkey, and Institute of Oriental Studies of the Russian Academy of Sciences, *The Turkey, Russia, Iran Nexus: Economic and Energy Dimensions—Proceedings of an International Workshop, Ankara, March 29, 2012* (Washington, D.C.: Center for Strategic and International Studies, 2012), 9, http://csis.org/files/publication/120529_Turkey_Russia_Iran_Nexus_Ankara_Workshop_Proceedings.pdf.

142. For the case that the deal was indeed bad for nonproliferation, see George Perkovich, "Global Implications of the U.S.-India Deal," *Dædalus* 139 (1) (Winter 2010): 20–31.

143. William Walker, "Nuclear Enlightenment and Counter-Enlightenment," *International Affairs* 83 (3) (May 2007): 433.

that the spread of nuclear weapons—even if they are not used—will undermine their national security in other ways. Their fears are often visceral but include falling victim to nuclear blackmail (i.e., being forced to make concessions under threat of nuclear attack) and adversaries' becoming emboldened after acquiring nuclear weapons.

The system for managing dual-use nuclear technology—as complex and multifaceted as it is—is focused narrowly on mitigating these "high-end" harms as they are posed by two potential agents: states that do not possess nuclear weapons; and sophisticated, well-funded, malevolent terrorist groups.

The nuclear nonproliferation regime, which aims to prevent further proliferation to states, represents Walker's "exceptional kind of cooperative politics." While non-nuclear-weapon states were not willing to forsake the use of nuclear energy for peaceful purposes, they did agree to construct a legally binding and nearly universal regime to reduce the risk that dual-use nuclear technology would be used in the development of nuclear weapons. This regime—for all its flaws and risks—represents humankind's most comprehensive attempt to manage any dual-use technology. It is essentially a transparency regime: states are permitted to conduct any nuclear activity, except the "manufacture" of nuclear weapons, provided they declare it and permit verification by the IAEA. Such verification is facilitated by both the relatively small number of weapon-usable fissile materials and the existence of inspection procedures that permit the diversion of declared nuclear materials to be detected reasonably reliably.

Restrictions on the trade in nuclear technology, materials, and equipment are a second component of the nonproliferation regime (although their effectiveness is gradually diminishing). They include unilateral and multilateral policies setting out the circumstances under which controlled knowledge or items can be exported, as well as unilateral and multilateral efforts, such as the Proliferation Security Initiative, to detect and interdict illicit transfers. Export controls and safeguards are connected: one purpose of the former is to provide the IAEA with information helpful to implementing the latter.

As exceptional as the nuclear nonproliferation regime is—in both its uniqueness and its success—it faces many serious stresses, including technical challenges such as detecting clandestine facilities and political challenges such as enforcement in the event a violation is detected. Few of these problems have easy answers, and there are many barriers to change. These include technical barriers, such as the inherent limitations of technology to detect secret nuclear activities; commercial barriers resulting from the potentially lucrative nature of nuclear exports; and political barriers, including the acrimony between nuclear-weapon states and non-nuclear-weapon states, as well as between technology holders and would-be recipients. These barriers make even incremental change difficult. Changes that would be more revolutionary—for example, rules to prevent the further spread of fuel-cycle technologies or an agreement to place all fuel-cycle facilities under multilateral or international control—are nonstarters. For the time being, the best opportunity for enhancing the nuclear nonprolifer-

ation regime, in this author's opinion, is for advanced states to develop internal procedures to assess how their domestic decisions to develop or use new nuclear technologies might affect proliferation dynamics globally.

While the nuclear nonproliferation regime developed from the top down—the passage of international agreements required national legislation and implementation—the nuclear security architecture developed from the bottom up. Efforts to prevent terrorist organizations or other unauthorized personnel from gaining access to nuclear facilities or acquiring nuclear material were originally a purely sovereign responsibility. Best practices include the development and periodic updating of design basis threats, physical protection to prevent unauthorized access, material control and accountancy to detect unauthorized removal, and effective response capabilities to recover material that has been removed.

Gradually, a patchwork of international measures has been developed to improve both national standards and the quality of implementation. These measures can be divided into four categories. First, a few legally binding instruments, such as the CPPNM and its amendment, as well as UNSCR 1540, impose legally binding standards in some areas. Second, best practice guides, such as INFCIRC/225, are an important but nonbinding way of plugging some of the remaining gaps. Third, various international assistance programs are also on offer, serving a wide variety of functions. The IAEA, through its International Physical Protection Advisory Service, provides peer reviews comparing a state's nuclear security system to internationally accepted best practice. National and regional centers of excellence are being set up to provide services such as training. Direct assistance with enhancing physical protection and material control procedures, removing high-risk materials, and converting HEU-fuelled research reactors to use LEU fuel is also available from multilateral coalitions and on a bilateral basis, most notably from the United States. Fourth, information-sharing initiatives, including the IAEA's Illicit Trafficking Database, have been created to warn states of potential threats. Information sharing is also a major purpose of the Proliferation Security Initiative.

Inspired, no doubt, by the nonproliferation regime, many nuclear security advocates are championing the idea of a comprehensive, legally binding, universal nuclear security treaty. Such a treaty would be a heavy diplomatic lift. The lack of a shared threat perception and fears that a nuclear security treaty would ultimately lead to technology denial would make garnering the support of many developing states difficult. Meanwhile, many developed states, worried that negotiations would be extremely difficult and carry a low chance of success, feel that their diplomatic capital might be better spent trying to effect more-incremental change. They are probably right. Because of the inevitable trade-off between high standards and universality, any treaty that was acceptable to a majority of states would, in all probability, lack the teeth necessary to combat the very real nuclear security problems that do exist.

In fact, the nuclear nonproliferation regime offers something of a false lead for nuclear security. Nonproliferation politics have become much more fractious since the NPT was concluded in 1968. While a majority of states still support the treaty, few feel that most others have acted in good faith. Most vociferously, the Non-Aligned Movement, while expressing concern about technology denial, argues that the nuclear-weapon states have failed to live up to their disarmament commitments. Meanwhile, although their public comments tend to be more measured, the United States and its partners are equally frustrated over the failure of many non-nuclear-weapon states to support efforts to bolster the nonproliferation regime. This acrimony has infected discussions of nuclear security; as desirable as isolating nuclear security from nonproliferation politically might be, doing so is simply not possible. Given this political reality, it is far from clear that fashioning a nuclear security regime in the mold of the nuclear nonproliferation regime is possible or that trying to do so would be constructive.

Chapter 2

Dual-Use Threats: The Case of Biological Technology

Elisa D. Harris

INTRODUCTION

In February 2001, the *Journal of Virology* published the results of a scientific experiment in which Australian researchers exploring contraceptive alternatives to pesticides for controlling the mouse population unexpectedly produced a lethal mousepox virus and, in the process, demonstrated how a new, highly virulent pathogen might be constructed.[1] This work might well have gone unnoticed by most people, other than interested scientists, had it not been for the fact that seven months later, terrorist attacks were carried out on the U.S. World Trade Center and the Pentagon and a series of letters containing high-grade anthrax spores were sent to selected U.S. media outlets and members of Congress. The latter events, which killed five and injured seventeen others, unleashed an epidemic of fear that terrorists would attack America again, only this time the weapon of choice would not be a commercial airliner but a biological agent that would cause death on a massive scale. Government officials and commentators alike warned that it was not a matter of whether bioterrorists would strike but of when.

Prior to September 11 and the anthrax letters, biological threats were seen largely through the lens of biosafety or nonproliferation—that is, ensuring that scientists' use of hazardous biological materials did not threaten human health or the environment, or preventing government-led programs aimed at developing and producing biological weapons. By the end of 2001, a new threat had been added to these traditional concerns: terrorist acquisition or use of

1. Ronald J. Jackson et al., "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75 (3) (February 2001): 1205–1210.

biological agents. Efforts to counter the theft, diversion, or malicious use of dangerous pathogens and toxins by terrorists came to be known as biosecurity.[2]

Over the past half century, many different governance measures have been adopted and still others proposed to prevent both accidental and deliberate releases of biological agents and the corresponding damage, human and financial, this would cause. These measures span multiple levels: international, national, local, and individual. They also take many forms: legally binding treaties, United Nations (UN) Security Council resolutions, and intergovernmental decisions; national laws and regulations; like-minded government policies; national and departmental policies; guidelines and standards; and scientific codes. Taken together, they help to form what some have called a "web of prevention."[3] But, like any web, there are gaps.

This chapter begins with a brief discussion of why governance of biological materials, equipment, and information is so inherently difficult. It then considers some of the most important governance measures that have been adopted at the international level, in the United States, and in other countries. These measures are grouped by their primary objectives: preventing the development and possession of biological warfare agents or weapons; controlling access to dual-use biological materials, equipment, or associated information that could be used for hostile purposes; promoting the safe and secure handling of pathogens and toxins inside and outside the laboratory; and ensuring that the risks from the most consequential types of biological research are properly identified, assessed, and mitigated before the work is carried out. The chapter then looks at two other types of governance measures that have been prominent in the dual-use biological technology debate, and concludes with a discussion of the key challenges confronting further efforts to mitigate dual-use risks in this area.

GOVERNANCE OF BIOLOGICAL TECHNOLOGY

As other studies have pointed out, governance of biological technology is inherently difficult.[4] First, most biological agents, such as bacteria and viruses, are living organisms that replicate, so policies that focus on inventory controls and accountability, especially monitoring the quantity of materials being stored, are problematic, as small seed stocks can later be used to produce large amounts of biological agent. Most biological agents can also be found in nature—in diseased soil or animals in the case of pathogens and in other living organisms in the case of toxins. While technical proficiency is required to obtain biological

2. Jonathan Tucker, "Preventing the Misuse of Pathogens: The Need for Global Biosecurity Standards," *Arms Control Today* 33 (5) (June 2003), http://www.armscontrol.org/act/2003_06/tucker_june03.

3. Brian Rappert and Caitriona McLeish, *A Web of Prevention: Biological Weapons, Life Sciences and the Governance of Research* (London: Earthscan, 2007).

4. See, for example, Tucker, "Preventing the Misuse of Pathogens."

materials from these natural sources, the fact that it can be done means that policies aimed at controlling access to dangerous pathogens or toxins can also be evaded.

Second, advances in science and technology are increasing the number of biological agents of potential concern, expanding the types of equipment relevant to their development and production, and broadening the range of facilities in which work with biological agents is occurring. During the Cold War, fewer than two dozen biological agents were developed and accepted into national biological weapons programs. However, advances in genetic sequencing and in synthetic biology are now making it possible to create an almost unlimited number of modified organisms, some of which may be more dangerous than existing biological agents, harder to detect, or capable of evading existing therapeutics.

Until a decade ago, efforts to control the acquisition of equipment that could be used to make biological agents focused on items such as high containment facilities, fermenters, specialized separators and filtration equipment, and aerosol test chambers, most of which were available in a relatively small number of countries. Today, modified organisms are being created more quickly and cheaply using sophisticated gene synthesis machines and reagents that are widely available. This work is being carried out in many countries and in diverse settings—in academic institutions, in industry and other private sector facilities, in government laboratories, and, in some cases, at sites where amateur scientists work without any institutional affiliation.

Third, governance of biological technology must also grapple with intangible technology—specifically, information or knowledge. This includes, for example, technical data necessary for the development or production of biological agents; it also includes the DNA sequence databases and design software available on the Internet that are central to the synthesis of modified or novel agents. And it includes the methods and results of research that are disseminated in multiple ways—in conversations among scientists, in email exchanges, in posters or presentations at scientific conferences, and in peer-reviewed publications.

Finally, each of these items—the biological materials, equipment, and related information—is used for legitimate purposes but can also cause harm, either accidentally or deliberately. Pathogens being studied for human or animal vaccines can escape from laboratories and sicken those they were designed to protect. Equipment used to understand the underlying biological properties of existing pathogens can also be directed toward enhancing the transmissibility or virulence of those pathogens for hostile applications. Information on the synthesis of an extinct pathogen like the 1918 Spanish flu virus can be used to bolster disease surveillance as well as to resurrect and disseminate this once-lethal threat. These characteristics have had a profound impact on efforts at every level to govern dual-use biological technology.

CURRENT STATE OF INTERNATIONAL GOVERNANCE

Many efforts have been undertaken at the international level to try to manage biological threats (see Table 1). These include treaty restrictions on the development and possession of biological weapons; multilateral initiatives aimed at preventing dual-use biological material, equipment, and information from being acquired for hostile purposes; and international guidelines and policies to ensure that pathogens and toxins are handled safely and securely.

Treaty Restrictions on Biological Weapons Development and Possession

During the 1960s, controversy over the use of herbicides and riot control agents by U.S. forces in Vietnam helped stimulate international interest in banning chemical and biological weapons. This ultimately led in 1972 to the conclusion of the Biological Weapons Convention (BWC), the first international treaty outlawing an entire class of weapons of mass destruction. From the outset, the BWC's terms acknowledged the dual-use nature of biological agents: instead of prohibiting biological *weapons* specifically, it committed parties never to "develop, produce, stockpile, or otherwise acquire or retain: microbial or other biological agents, or toxins . . . of types and in quantities *that have no justification for prophylactic, protective or other peaceful purposes*," as well as "weapons, equipment or means of delivery designed to use such agents or toxins *for hostile purposes*."[5] This language also ensured that the BWC's fundamental prohibitions would apply to all future scientific and technological developments in the life sciences and related fields, including in the nascent field of biotechnology. BWC parties have reaffirmed this view regarding the scope of application of the BWC at each successive review conference since the convention entered into force in 1975.

In addition to prohibiting the development and possession of biological weapons, the BWC also obligates its parties not to transfer to others and not to assist any state in producing or acquiring biological agents or toxins (as well as weapons, equipment, or delivery means) for other than peaceful purposes. At the same time, the convention commits its parties to facilitate the fullest possible exchange of materials, equipment, and information for using biological agents and toxins for peaceful purposes and to avoid hampering international cooperation in such activities. This tension between the nonproliferation and assistance provisions of the BWC has been a major source of controversy between developed and developing countries since the earliest days of the convention.

The biggest weakness of the BWC, however, is the absence of meaningful mechanisms for ensuring that countries comply with their obligations. The implications of this failure became apparent in the late 1980s as reports began to emerge from Soviet biological weapons scientists who had defected to the West.

5. "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction" (1972), http://www.opbw.org/convention/documents/btwctext.pdf; emphasis added.

Table 1: International Governance of Biological Technology

Measure	Date	Current Participants	Purpose	Comments
Biological Weapons Convention	1975	173 parties, 9 signatories	Ban biological agents, toxins for other than peaceful purposes	Legally binding; no verification; tension between nonproliferation and assistance provisions
WHO Biosafety Manual	1983	194 countries	Prevent unintentional exposure to pathogens/toxins; safe use of recombinant DNA technology	Global health authority; focus on guidelines to assist members; recommendations nonbinding
WHO Biosecurity Manual	2004		Prevent intentional misuse	
WHO Responsible Life Sciences Research Guidance	2010		Promote responsible life sciences research	No guidelines for research oversight
OECD rDNA Handbook	1986	34 countries	Promote safety of rDNA work	Multilateral organization, limited membership; recommendations nonbinding
OECD Biosecurity Guidance	2001		Provide biosecurity guidelines	
Australia Group	1992	42 countries plus European Commission	Harmonize national controls on biological materials and equipment	Informal body; political commitment
UNSCR 1373	2001	193 countries	Share information on WMD terrorism	Legally binding; no provisions for implementation
UNSCR 1540	2004	193 countries	Enact and enforce controls on biological materials, equipment, information to prevent terrorist acquisition	Legally binding; implementation of biological commitments unclear
G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction	2002	28 countries	Commit $20 billion over 10 years to prevent terrorist acquisition of WMD/materials/info from FSU	Multilateral initiative; political not legal commitment; delay in meeting initial goals
	2011		Added implementation of UNSCR 1540, pathogen security and lab safety	Russia ousted in 2014 after Crimea annexation

Measure	Date	Current Participants	Purpose	Comments
Proliferation Security Initiative	2003	103 countries	Interdict shipment of WMD and related materials to states/nonstate actors of concern	Multilateral initiative; no implementing body; political not legal commitment
INTERPOL Bioterrorism Prevention Program	2006 2014	190 member states	Strengthen criminal and administrative laws to prevent terrorist acquisition of biological agents; Promote security/safety of biological materials and emerging technology	International police organization; recommendations nonbinding
Screening of Gene Sequence Orders	2009	Major U.S. and European suppliers	Screen sequence orders to prevent customers from creating dangerous biological agents	Voluntary supplier initiative

These scientists revealed that Moscow had not only maintained its biological weapons program after the conclusion of the BWC but had expanded it into the largest and most sophisticated program in the world. At its peak, the Soviet program involved some 65,000 scientists, technicians, and other workers hidden in dozens of facilities operated by the KGB, the Soviet Academy of Sciences, the Soviet Academy of Medical Sciences, and the Ministries of Defense, Agriculture, Health, and Chemical Industry. Much of this illegal biological weapons program was hidden in plain sight in facilities conducting research and development (R&D) for pharmaceutical, industrial, and other civilian purposes. The real mission of the facilities operated by Biopreparat, as the civilian side of the Soviet biological weapons program was called, was R&D on human pathogens, particularly the development of antibiotic- and vaccine-resistant biological agents.[6]

The Soviet Union was not, however, the only country believed to have a biological weapons program. In the late 1980s, U.S. officials began to speak publicly about a broader proliferation problem, claiming that the number of countries with biological weapons programs had increased from four to ten in the years since the BWC had been completed. In addition to the Soviet Union, the other countries that were identified as having biological weapons programs were China, Egypt, Iran, Iraq, Libya, North Korea, South Africa, Syria, and Taiwan, almost all of which had either signed or ratified the convention.[7] Biological weapons proliferation became an even more salient issue in the run-up to the 1991 Gulf War because of fears that Saddam Hussein would authorize the use of biological (or chemical) weapons against the coalition of military forces that had been assembled to oust Iraqi troops from Kuwait. Although this did not come to pass, UN inspectors confirmed in the years after the war that Iraq had developed and produced biological weapons during the 1980s and that biological materials and equipment from Western companies had facilitated the Iraqi program.

In the face of mounting concerns about the proliferation of biological weapons, BWC parties agreed in 1991 to study potential verification measures for the convention and in 1994 created an ad hoc group with a carefully defined mandate: to consider appropriate measures, including *possible* verification measures, to be included *as appropriate* in a legally binding protocol to strengthen the BWC. The debate over the mandate foreshadowed the positions taken by the parties in the protocol negotiations: the European Union (EU) and moderate nonaligned countries supported a variety of data declaration and on-site inspection requirements; China and the radical nonaligned countries pressed for commitments on technical assistance for developing countries and the elimination of export controls; and Russia tried to

6. For the most authoritative study on the Soviet program, see Milton Leitenberg and Raymond A. Zilinskas, *The Soviet Biological Weapons Program: A History* (Cambridge, Mass.: Harvard University Press, 2012).

7. See Milton Leitenberg, *Assessing the Biological Weapons and Bioterrorism Threat* (Carlisle, Pa: U.S. Army War College, 2005).

narrow the scope of the BWC's prohibitions and thus widen the definition of permitted activities. The U.S. government was divided: the White House was supportive of legally binding transparency measures to increase the risk and cost of cheating, whereas government departments were determined to limit the protocol's impact on sensitive biodefense and threat assessment activities and on the U.S. biotechnology and pharmaceutical industries. In July 2001, the new George W. Bush administration, whose officials had an antipathy to arms control in general and to BWC verification in particular, officially rejected the draft protocol that had been negotiated.

Following the September 11 attacks and the anthrax letters, the United States proposed, as an alternative to continuing the protocol negotiations, that state parties hold short intersessional meetings each year to exchange information on biosecurity and global health security issues, including controls on dangerous pathogens, laboratory biosafety and biosecurity, and disease surveillance. Discussions on these and related issues have continued for more than a decade, with few tangible results. Currently 173 states are party to the BWC (i.e., have both signed and ratified the convention). Nine, including Egypt and Syria, are signatories only, and fifteen, including Israel, have neither signed nor ratified the convention.

Multilateral Efforts to Control Access to Biological Material, Equipment, and Information

Since the early 1990s, a variety of international initiatives have been undertaken to try to prevent dual-use biological material, equipment, and information from being acquired for hostile purposes. Some of these initiatives have been truly international in scope, though most have been what more accurately could be called "multilateral," since they have involved smaller groups of like-minded countries.

The first of these initiatives was the harmonization of national controls on biological-related exports by the Australia Group (AG), an informal export control coordinating body that was organized by the Australian government after Iraq's use of chemical weapons in the Iran-Iraq War. In December 1992, the twenty-two members of the AG agreed to control the export of fifty-three human and animal pathogens, ten toxins, and seven types of equipment that could be diverted to the production of biological weapons.[8] Since that time, the AG's membership has expanded to forty-two countries (plus the European Commission), its control list for human and animal pathogens has increased to ninety microorganisms and nineteen toxins, and its equipment list has grown to include nine categories of items. The AG also has added a plant pathogens control list that as of early 2016 comprised eighteen microorganisms. Genetic elements and genetically modified organisms that contain nucleic acid sequences associated with the pathogenicity of any of the listed agents are included under

8. U.S. Arms Control and Disarmament Agency, *The Australia Group*, Occasional Paper (Washington, D.C.: U.S. Arms Control and Disarmament Agency, May 1993).

the AG controls. Items not specifically on the AG control lists but for which there is information that they may be used for biological weapons purposes also are to be controlled by member states. In addition to implementing these "catch-all" controls, AG members also have agreed that if one member denies a specific export license, the others will consult with that member before deciding whether to approve the same transaction.[9]

After September 11 and the anthrax letters, international as well as multilateral efforts to prevent the spread of biological weapons capabilities focused largely on terrorists and other nonstate actors. Following the 2001 attacks, the UN Security Council unanimously adopted UN Security Council Resolution (UNSCR) 1373, which, among other things, obligated all UN member states to enhance information sharing on illegal transfers of biological and other potentially deadly materials that could be used by terrorists groups. No modalities were provided, however, for implementing this commitment. Three years later, the Security Council unanimously adopted UNSCR 1540, committing all UN member states to enact and enforce laws and other measures against the spread of biological and other weapons of mass destruction and delivery means, including controls on related materials, equipment, and technology, to terrorists or other nonstate actors. Under this resolution, UN members are required to report to a dedicated UN committee on the measures they have taken or intend to take to implement these obligations. As of December 2014, 173 member states had submitted implementation reports; however, most of the measures reported were in the nuclear or chemical fields.[10]

Another initiative targeted against terrorist acquisition of biological and other weapons is the G8 Global Partnership against the Spread of Weapons and Materials of Mass Destruction. Under this program, which was created in June 2002, the G8 industrialized countries (Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States) committed to raise up to $20 billion over ten years to fund activities aimed at preventing terrorists or the states that support them from gaining access to weapons, material, and information that could be used in biological or other weapons of mass destruction. Much of the Global Partnership's initial work was focused on the former Soviet Union, where it funded over four thousand research projects and related activities aimed at redirecting former Soviet scientists, including biological weapons

9. Although the AG's focus remains national chemical and biological weapons programs, in 2014 it acknowledged the risk of diversion to nonstate actors, agreeing that members should consider the possibility of terrorist acquisition prior to approving the export of any AG-controlled item. See "The Australia Group," 2007, http://www.australiagroup.net/en/index.html.

10. For the most recent implementation report, see Oh Joon, "Letter Dated 31 December 2014 from the Chair of the Security Council Committee Established Pursuant to Resolution 1540 (2004) Addressed to the President of the Security Council," S/2014/958, United Nations Security Council, December 31, 2014, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2014/958.

scientists, toward sustainable civilian activities.[11] In May 2011, partly because of delays in meeting its original financial goal, the G8 decided to extend the Global Partnership beyond its original ten-year mandate. The G8 also agreed to expand membership in the initiative and to broaden efforts in certain priority areas, including redirecting former biological and other weapons scientists, assisting in implementation of UNSCR 1540, and working to secure dangerous pathogens and improve laboratory biosafety. Although Russia was ousted from the G8 following its annexation of Crimea in 2014, the twenty-eight remaining members of the Global Partnership appear committed to pursuing this broader agenda.[12]

In the years immediately after September 11, the United States and ten other countries also launched the Proliferation Security Initiative (PSI), which seeks to stop shipments of weapons of mass destruction, their delivery means, and related dual-use material to both state and nonstate actors of proliferation concern. Although countries like China, Iran, and North Korea view the PSI as a violation of international law protecting freedom of the seas, 103 countries, including Russia, the Republic of Korea, and many major international shipping nations, have endorsed the PSI and committed to abide by its founding principles: not to transfer proliferation-related items to countries of concern; to cooperate in searches of suspected cargoes on their own vessels or aircraft or on other vessels passing through their territory; and to share information quickly on suspicious activities that might require interdiction. Participants are expected to put in place the necessary legal authorities and operational capabilities to meet these commitments. Although the PSI has no implementing body, twenty-one of the most active PSI members exchange information and coordinate activities through an operational experts group. In May 2013, on the tenth anniversary of the founding of the initiative, seventy-two PSI participants held a high-level political meeting where they pledged to hold PSI interdiction exercises on a more regular basis, promote treaties criminalizing the illegal trade in weapons of mass destruction (WMD)–related items; cooperate in enhancing interdiction capabilities; and expand the PSI's global outreach to other countries.[13] Information is not available, however, about the PSI's effect on the illegal trade in biological or other weapons-related materials.

11. G8 Global Partnership, "Assessment and Options for Future Programming: G8 Summit, May 26–27, 2011, Deauville, France," Partnership for Global Security, http://www.partnershipforglobalsecurity-archive.org/Official%20Documents/G-8%20Global%20Partnership/620201181141AM.html.

12. Bonnie D. Jenkins, "The Future Role of the G-8 Global Partnership: Combatting Weapons of Mass Destruction," Policy Analysis Brief, Stanley Foundation, June 2010; "The United States Chairmanship of the Global Partnership in 2012," U.S. Department of State, n.d., http://www.state.gov/t/isn/gp2013/; and United Kingdom, "2010 to 2015 Government Policy: Weapons Proliferation," May 8, 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-weapons-proliferation/2010-to-2015-government-policy-weapons-proliferation#appendix-5-global-partnership.

13. Arms Control Association, "The Proliferation Security Initiative (PSI) at a Glance," updated June 2013, http://www.armscontrol.org/factsheets/PSI.

INTERPOL, the 190-member-country international police organization, also became active on bioterrorism after the September 11 terrorist attacks and anthrax letters. INTERPOL's initial work focused largely on assisting member states to prepare for and respond to a possible bioterrorist attack. In 2006, however, under the auspices of its Bioterrorism Prevention Program, the organization launched a new project aimed at helping countries assess, strengthen, and enforce their criminal and administrative laws in order to prohibit the acquisition, transfer, and use of biological materials for hostile purposes. Little is known, however, about the impact of this effort or of a more recent INTERPOL project known as Operation S3OMMET. Under this 2014 initiative, INTERPOL announced it would work with relevant regional and international partners to raise awareness among law enforcement and public health officials, biosafety officers, and research scientists in key regions on how to improve the safety and security of dual-use biological materials and related emerging technologies so as to prevent unauthorized access to them by those who would do harm.[14]

Governments have not been the only actors pursuing initiatives to address bioterrorism concerns. In the mid-2000s, a number of gene synthesis companies in the United States and Europe voluntarily began to screen customer orders to ensure that the sequences they supplied could not be used to make high-risk pathogens. But the industry did not adopt a uniform approach, and some companies declined to screen at all. To help develop a more harmonized approach, various gene synthesis companies began to form international consortiums to promote greater attention to biosecurity, including the screening of orders. In 2009, the International Association Synthetic Biology, a group of largely German commercial suppliers, developed a proposal for screening sequence and customer orders. A few months later, five of the world's leading gene synthesis companies formed a competing group, the International Gene Synthesis Consortium, to develop their own screening proposal. In the end, both industry groups, which together represented most of the global gene synthesis industry, agreed to screen all synthetic gene orders they received not only for sequences of known high-risk pathogens but also for reasonably similar sequences that could be used to create novel pathogens. They also agreed to screen all customers who placed orders, to maintain sequence and customer records, and to report potentially problematic orders to the appropriate authorities.[15] Some suppliers wanted to go even further, arguing that their voluntary approach should be replaced by mandatory screening requirements in Europe and the United States, backed by strong enforcement action, but this has not been done.[16]

14. For information on INTERPOL's bioterrorism activities, see "CBRNE," INTERPOL, n.d., http://www.interpol.int/Crime-areas/Terrorism/CBRNE/Biological-threats.

15. Jonathan B. Tucker, "Double Edged DNA: Preventing the Misuse of Gene Synthesis," *Issues in Science and Technology* XXVI (3) (Spring 2010): 23–32, http://issues.org/26-3/tucker-2/.

16. Jeremy Minshull and Ralf Wagner, "Preventing the Misuse of Gene Synthesis," letter to the editor, *Nature Biotechnology* 27 (9) (September 2009): 800–801.

International Measures Governing the Handling and Use of Biological Agents

One of the earliest international initiatives focused on the handling of dual-use biological materials was the publication of a laboratory biosafety manual by the World Health Organization (WHO) in 1983. This manual provided guidance for WHO member states on physical containment principles, technologies, and practices to prevent *unintentional* exposure to or release of biological materials. Following September 11 and the anthrax letters, WHO began to address the issue of *intentional* biological threats, releasing in 2006 a separate volume on laboratory biosecurity, including guidance for the protection, control, and accountability of biological materials.[17] As the word implies, the guidance in these documents was not binding on WHO member states.

In parallel with its work on laboratory biosafety and biosecurity, WHO also began to examine the risks and opportunities of advances in the life sciences for global health security under a broader project on responsible life sciences research. In a report published in 2010, WHO recommended investing in three pillars that promote public health—research excellence, ethics, and laboratory biosafety and biosecurity—and provided a self-assessment questionnaire for public health officials, laboratory managers, and scientists to use to evaluate their strengths and weaknesses in these areas. This approach was premised on the belief that one of the most effective ways of preparing for deliberately caused disease is to strengthen public health measures for natural and accidental disease outbreaks. It also reflected the view that individual countries were in the best position to determine how to promote the safety and security of their biological research activities. The latter was a departure for the organization, which had previously issued international guidelines on both biosafety and biosecurity for member states.[18]

Like WHO, the Organisation for Economic Co-operation and Development (OECD) also has played a role in encouraging international harmonization of guidelines and regulations related to the handling of biological materials. In 1986, for example, the OECD issued a handbook on *Recombinant DNA Safety Considerations* for industrial, agricultural, and environmental applications.[19] In 2001, the OECD began to link various government, industry, and academic facilities that store, test, or use biological materials into a global exchange network of what it called biological resource centers (BRCs). To facilitate the sharing of biological agents among its members, the OECD also developed

17. For the biosafety manual, see World Health Organization, *Laboratory Biosafety Manual*, 3rd ed. (Geneva: WHO, 2004), http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_CSR_LYO_2004_11/en/. For the biosecurity guidance, see World Health Organization, *Laboratory Biosecurity Guidance* (Geneva: WHO, 2006), http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf.

18. World Health Organization, *Responsible Life Sciences Research for Global Health Security: A Guidance Document* (Geneva: WHO, 2010), http://www.who.int/csr/resources/publications/HSE_GAR_BDP_2010_2/en/.

19. Organisation for Economic Co-operation and Development, *Recombinant DNA Safety Considerations* (Paris: OECD, 1986), http://www.oecd.org/sti/biotech/40986855.pdf.

and issued biosecurity guidelines to prevent unauthorized access to the culture collections and other biological resources of the BRCs, including procedures for risk assessment and management, personnel security and training, and material controls. As with many of the other multilateral initiatives, the OECD's efforts apply only to its members—thirty-four as of early 2016—and are nonbinding.[20]

CURRENT STATE OF GOVERNANCE IN THE UNITED STATES

In the United States, a wide range of laws, regulations, policies, and guidelines have been adopted in an effort to prevent biological materials, equipment, or information from causing harm. For many years, most of these measures focused on ensuring domestic implementation of the BWC's prohibitions on biological weapons development and possession, trying to prevent the spread of biological weapons to other countries, or promoting the safe handling and use of biological materials. After September 11 and the anthrax letters, many of these measures were broadened to address concerns that terrorists or other non-state actors might seek to acquire or use biological weapons (see Table 2). An unprecedented debate also began among U.S. scientists, government officials, security experts, and other stakeholders over how to prevent the accidental or deliberate misuse of advances in life sciences research—a debate that continues to this day (see Table 3).

U.S. Restrictions on Biological Weapons Development and Possession

Although the United States played a major role in the conclusion of the BWC, it did not adopt domestic legislation outlawing the development and possession of biological weapons until nearly a decade and a half after the BWC entered into force. Under the Biological Weapons Anti-Terrorism Act of 1989, it became a crime to *knowingly* develop, produce, possess, or transfer biological agents, toxins, or delivery systems *for use as a weapon* or to assist another country or organization to do so. The act provided for criminal penalties against those who engage in prohibited activity but puts the burden of proof on the government to demonstrate hostile intent.[21]

In April 1996, following the Oklahoma City bombings and the acquisition of plague cultures through the mail by a member of the neo-Nazi organization Aryan Nation, the U.S. Congress expanded the scope of activities subject to criminal penalties under the 1989 law from *knowingly* developing, producing,

20. Organisation for Economic Co-operation and Development, *OECD Best Practice Guidelines on Biosecurity for BRCs* (Paris: OECD, 2007), http://www.oecd.org/sti/biotech/38778261.pdf.

21. *Biological Weapons Anti-terrorism Act of 1989*, Pub. L. 101–298, 104 Stat. 201 (1990). For a discussion of the legislation, see Ronald Atlas, Kenneth I. Berns, Gail Cassell, and Janet Shoemaker, "Preventing the Misuse of Microorganisms: The Role of the American Society for Microbiology in Protecting against Biological Weapons," *Critical Reviews in Microbiology* 24 (3) (February 1998): 273–280.

Table 2: U.S. Governance of Biological Weapons Development and Biological Materials Access and Use

Measure	Date	Title	Purpose	Comments
Federal Guidance	1976	*NIH Guidelines for Research Involving Recombinant DNA Molecules*	Outline lab practices, equipment, facilities for safety of rDNA research	Voluntary; applied only to rDNA research at institutions with NIH rDNA funding
Statute	1976	Arms Export Control Act	Control military biological exports	Legally binding; State Dept. license required
Statute	1979	Export Administration Act	Control export of dual-use biological agents	Legally binding; Commerce Dept. license required except for Australia Group/similar countries
Federal Guidance	1984	HHS *Biosafety in Microbiological and Biomedical Laboratories* Manual	Outline lab practices, equipment, facilities for laboratory biosafety	Voluntary
	2009		Added security, personnel and other aspects of laboratory biosecurity	Select agent facilities and federal contractors/grantees required to follow
Statute	1989	Biological Weapons Anti-Terrorism Act	Prohibit "knowing" development and possession of agents, toxins, delivery systems for use as a weapon	Legally binding; implemented BWC in United States 14 years after ratification; included criminal penalties
Executive Actions	1990	EO 12735; Enhanced Proliferation Control Initiative	Expand controls on bioweapons-related exports	Included dual-use equipment and other exports that could facilitate weapons development or use
Statute	1991	Soviet Nuclear Threat Reduction Act (Nunn-Lugar Cooperative Threat Reduction Program)	Prevent proliferation by eliminating Soviet nuclear, chemical, and biological capabilities	Dismantled weapons facilities, redirected scientists, secured pathogens, strengthened facility safety and security
	2007		Prevent terrorist acquisition NBC capabilities	Geography and scope expanded to include countries outside former SU, biosafety & biosecurity

Measure	Date	Title	Purpose	Comments
Army Guidance	1993	Biological Defense Safety Program	Prescribe safety requirements for biological agent RDT&E	Applied to Army, contractors, subcontractors
Statute	1996	Antiterrorism and Effective Death Penalty Act	Expand BWC Act to "attempts, threats or conspiracies"; add genetically engineered items; control transfers of human pathogens	Legally binding; regulations required: select agent list of human pathogens by CDC/HHS; disclosure of agent transfers; registration of transferring/receiving facilities
Statute	2001	USA PATRIOT Act	Prohibit biological agents, toxin, or delivery systems not for peaceful purposes and possession by "restricted persons"	Legally binding; shifted burden from government to suspect to prove intent
Department Policy	2001	DOD Directive 2060	Establish process for reviewing biological research for BWC compliance	No special attention to dual-use research
	2005	DHS Management Directive 6300	Establish process for reviewing biological research and other activities for BWC and regulatory compliance	Special scrutiny of certain dual-use research to ensure BWC compliance
Statute	2002	Public Health Security and Bioterrorism Preparedness and Response Act	Strengthen select agent controls by adding: facilities that possess/use select agents, personnel checks, facility inspections; regulate select agent research	Legally binding; parallel requirements for animal and plant agents by USDA; research oversight only of proposals subject to NIH approval; compliance problems in early years
Army Guidance	2008	Biological Surety	Increase safety and security of work with biological agents	Applied to Army, contractors, subcontractors; begun after 9/11 but not implemented for 7 years
Federal Guidance	2010	Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA	Advise commercial gene synthesis suppliers on screening sequence and customer orders	Voluntary; limited to select agents; weaker than industry-initiated screening protocols
Regulations	2012	Revised Select Agent Regulations	Strengthen pathogen controls by focusing on greatest threats; strengthen personnel reliability/physical security	Legally binding; removed 22 agents/toxins; added 3 viruses; designated 11 as Tier 1 (greatest risk); no official information on compliance

Table 3: U.S. Governance of Biological Research

Measure	Date	Title	Purpose	Comments
Federal Guidance	1976	*NIH Guidelines for Research Involving Recombinant DNA Molecules*	Ensure review and approval of rDNA research	Voluntary; applied only to rDNA research at institutions with NIH rDNA funding; IBCs/IRBs quickly replace RAC oversight; post-9/11 survey shows scores of institutions in noncompliance
	2010	*NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules*	Expanded to synthetic nucleic acid molecules to address biosecurity concerns	
Statute	2002	Public Health Security and Bioterrorism Preparedness and Response Act	Regulate select agent research	Legally binding; research oversight only of limited number of proposals subject to NIH approval; compliance problems in early years
CDC Guidance	2007	Oversight and Clearance of Dual-Use Research of Concern	Review intramural research using proposed NSABB framework for DURC	Voluntary; predates 2012 U.S. government-wide policy; left DURC determination to researchers; criterion subjective and vague
NIH Guidance	2008	NIH Dual-Use Screening Program	Review intramural research using proposed NSABB framework for DURC	Voluntary; predates 2012 U.S. government-wide policy; left DURC determination to researchers; criterion subjective and vague
U.S. Government Policy	2012	U.S. Government Policy for Oversight of Life Sciences Dual Use Research of Concern	Review unclassified life sciences research conducted or funded by U.S. Government for DURC	Announced 5 years after NSABB DURC proposal; applies only to research with 15 select agents; excluded privately funded and classified research; used subjective NSABB criterion
HHS Guidance	2013	HHS Framework for Funding Decisions about HPAI H5N1 Research	Strengthen oversight of H5N1 proposals by reviewing for DURC, scientific benefit, safety and security risks; later extended to H7N9 virus	Complicated, lengthy process with multiple review levels

Measure	Date	Title	Purpose	Comments
U.S. Government Policy	2014	Deliberative Process for Gain of Function Research	Develop new U.S. government policy for conduct and funding of GOF research	Focus on research with highly transmissible pathogens—influenza, SARS, MERS viruses; accompanied by pause in funding new studies, call for voluntary pause on ongoing work
U.S. Government Policy	2014	U.S. Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern	Outline institutional responsibility to review unclassified life sciences research for DURC if institution receives U.S. government life sciences research funding	Announced 7 years after NSABB DURC proposal; applies only to research with 15 select agents; excludes research at facilities not receiving U.S. government funding for life sciences research and classified research; uses subjective NSABB criterion; makes PI responsible for initiating DURC review

possessing, or transferring biological agents for use as a weapon to *attempts, threats, or conspiracies* to do so. The April 1996 Antiterrorism and Effective Death Penalty Act, which was the source of this broader criminalization provision, also expanded the definition of a biological agent to include genetically engineered products or components thereof.[22]

After September 11 and the anthrax letters, the United States modified these provisions on criminalization still further, making it a crime under the October 2001 USA PATRIOT Act for anyone to knowingly possess any biological agent, toxin, or delivery system *not reasonably justified for prophylactic, protective, bona fide research, or other peaceful purposes.* Of note, the bill shifted the burden of proof—instead of the government having to prove hostile intent, suspects now had to demonstrate that their activities were for peaceful purposes. The bill also criminalized the possession, transportation, or receipt of particularly dangerous pathogens, known as select agents, by certain restricted persons, including illegal aliens, individuals from terrorist-list countries, fugitives from justice, and individuals who are under indictment or have been imprisoned for more than one year.[23] The Federal Bureau of Investigation's (FBI) Weapons of Mass Destruction Directorate, a law enforcement unit dedicated to preventing terrorism and proliferation involving biological and other weapons of mass destruction, was given responsibility for enforcement.[24]

As U.S. government biodefense research expanded following September 11, U.S. government agencies also put in place formal review processes to ensure that their biological research activities complied with the BWC. Since 2001, for example, the Department of Defense (DOD) has required all biological-based activities, which include both classified and unclassified biodefense research, conducted at DOD facilities or funded by DOD to be reported annually to the department and reviewed by its BWC Compliance Review Group. Dual-use research does not, however, receive special attention in the DOD BWC compliance review process.[25]

22. *Antiterrorism and Effective Death Penalty Act of 1996*, Pub. L. 104–132, 110 Stat. 1214 (1996), sec. 511. The CDC role in implementing this legislation builds upon the responsibility given to CDC in 1971 to help ensure the safety of interstate shipments of infectious substances. See Gerald Epstein, "Controlling Biological Warfare Threats: Resolving Potential Tensions among the Research Community, Industry and the National Security Community," *Critical Reviews in Microbiology* 27 (4) (2001): 323.

23. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Pub. L. 107–56 (2001), sec. 817.

24. *Ten Years after 9/11 and the Anthrax Attacks: Protecting against Biological Threats: Hearing before the Committee on Homeland Security and Governmental Affairs, United States Senate, One Hundred Twelfth Congress, First Session*, 112th Cong. (2011) (statement of Vahid Majidi, Assistant Director, Weapons of Mass Destruction Directorate, Federal Bureau of Investigation), http://www.hsgac.senate.gov/hearings/ten-years-after-9/11-and-the-anthrax-attacks-protecting-against-biological-threats.

25. Although the DOD BWC compliance policy dates to 1992, a more structured process does not appear to have been adopted until 2001. Center for Arms Control and Non-proliferation, *Ensuring Compliance with the Biological Weapons Convention, Meeting Report* (Washington, D.C.: Center for Arms Control and Non-proliferation, July 2009).

In 2005, the Department of Homeland Security (DHS) issued its own compliance review policy for DHS biological research, development, and acquisition activities, including biodefense research. The DHS policy covers both treaty compliance and compliance with U.S. regulatory requirements, including those involving biosafety and the security of select agents. In contrast to DOD, DHS explicitly scrutinizes certain categories of dual-use biological research to ensure that it complies with U.S. BWC obligations. Under the DHS approach, all relevant projects must be submitted to the DHS Compliance Assurance Program office, which is responsible for reviewing and assessing the projects prior to their consideration by the department's Compliance Review Group (CRG). The CRG, which is chaired by the deputy secretary of DHS, must approve all such projects before they can proceed.[26]

U.S. Measures to Control Access to Biological Materials, Equipment, and Information

For many years, the United States has undertaken a number of initiatives to try to prevent countries of proliferation concern from acquiring material, equipment, and information that could be used to develop and produce biological weapons. Under the authority of the Export Administration Act (EAA), the Commerce Department began in the 1980s to require a license for the export of several categories of biological agents, including genetically modified agents. Following revelations that U.S. and other Western companies had supplied dual-use chemical and biological materials and equipment to Iraq's weapons programs, the United States expanded its dual-use export controls under Executive Order 12735 and the Enhanced Proliferation Control Initiative. Among other things, these 1990 measures extended U.S. export controls to dual-use chemical and biological equipment and technology as well as to any other proposed export that might be related to the acquisition or use of chemical or biological weapons. Today the biological provisions of the Commerce Control List include human, plant, and animal pathogens and toxins controlled by the AG, select agent pathogens, and genetic elements for those controlled agents and toxins. Consistent with the AG, the United States also controls the export of nine types of dual-use equipment that could be used to handle biological agents. Members of the AG and other countries that have entered into agreements to control dual-use biological material and equipment are exempt from the EAA's licensing requirement.[27]

26. Ibid.

27. White House, Office of the Press Secretary, "Executive Order 12735: Chemical and Biological Weapons Proliferation," November 16, 1990; and White House, Office of the Press Secretary, "Fact Sheet on Enhanced Proliferation Control Initiative," December 13, 1990. For current information on U.S. dual-use biological export controls, see Department of Commerce, Bureau of Industry and Security, "Chemical and Biological Controls," updated January 2014, http://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/16-policy-guidance/product-guidance/122-chemical-and-biological-controls.

Under the Arms Export Control Act, the State Department has similar authority to control military biological exports. Biological agents and biologically derived substances specifically developed, configured, adapted, or modified for the purpose of increasing their capability to produce casualties in human beings or livestock, to degrade equipment, or to damage crops are controlled as "significant military equipment" on the United States Munitions List and require a license for export. Both the State and Commerce Departments also control the transfer of specific technical information necessary for the development, production, or use of biological weapons to foreign nationals in the United States under a category called "deemed exports."

In the early 1990s, following the collapse of the Soviet Union, the United States sought to prevent the proliferation of former Soviet nuclear, chemical, and biological weapons capabilities to other countries through the Nunn-Lugar Cooperative Threat Reduction (CTR) program. Threat reduction activities related to biological weapons have continued since that time and, after September 11 and the anthrax letters, expanded from Russia and other former Soviet republics to the Middle East, Southeast Asia, and Africa. This multiagency U.S. effort involving the Defense, State, Energy, and Homeland Security Departments has dismantled former biological weapons facilities, redirected former weapons scientists from illicit to legitimate activities, secured collections of dangerous pathogens, carried out biosafety and biosecurity upgrades at research laboratories, and provided biosafety and biosecurity training to scientists and other laboratory personnel. Many of these projects have been spearheaded by DOD, where biological threat reduction has grown from less than 10 percent of the threat reduction budget in the 1990s to more than 60 percent today. This growth is a reflection of the expansion of the CTR program's biological mission, from preventing the spread of biological weapons capabilities from the former Soviet Union to promoting biological nonproliferation, biosafety, and biosecurity around the globe.[28] Much of the proliferation threat from the former Soviet biological weapons program has been eliminated; however, residual concerns remain about Russia's handful of still-secret military biological facilities and about the future of its nonmilitary biological facilities since Russia ended its participation in the CTR program in 2014.[29]

U.S. efforts to control access to dual-use biological materials, equipment, and information have not, however, been motivated only by proliferation concerns. Fears of bioterrorism also have led to efforts to tighten controls on domestic access to biological weapons–related items. Perhaps the most important of these is the select agent program, which was established by the April

28. Mary Beth Nikitin and Amy Wolff, *The Evolution of Cooperative Threat Reduction: Issues for Congress*, CRS Report for Congress, R43143 (Washington, D.C.: Congressional Research Service, June 2014), https://www.fas.org/sgp/crs/nuke/R43143.pdf.

29. Richard Weitz, "Russian-US Cooperative Threat Reduction beyond Nunn-Lugar and Ukraine," Arms Control Association, July 2, 2014, https://www.armscontrol.org/act/2014_0708/Features/Russian-US-Cooperative-Threat-Reduction-Beyond-Nunn-Lugar-and-Ukraine.

1996 antiterrorism law to strengthen the security of biological agents that could pose a severe threat to human health. Regulations to implement the new law were published by the Centers for Disease Control and Prevention (CDC) in October 1996 and took effect in April 1997 and included:

- a select agent list of approximately forty human pathogens and toxins, including genetic elements and genetically modified organisms associated with those agents;
- a registration requirement for any facility that seeks to *transfer* or *receive* select agents, including certification to the CDC that the facility and its laboratories meet the requisite biosafety standards; and
- a disclosure obligation, including information from both the transferring and receiving facility on the type and amount of agent requested and the proposed use.[30]

After September 11 and the anthrax letters, the U.S. Congress extended these controls over facilities that *transfer* or *receive* select agents to cover facilities that *possess* and *use* them as well, and added new personnel reliability and security requirements. Under the May 2002 Public Health Security and Bioterrorism Preparedness and Response Act, anyone who was to have access to select agents was now required to register with the Department of Health and Human Services (HHS) and undergo a Justice Department background check, known as a security risk assessment. The act also directed HHS to maintain a national database of registered facilities, persons, and the select agents they possess or are transferring and to conduct inspections of relevant facilities. Civil and criminal penalties can be imposed on facilities for failing to register or for transferring select agents to an unregistered facility. The May 2002 bioterrorism law also required the secretary of agriculture to establish parallel registration, security, record keeping, and inspection requirements to enhance the security of biological agents and toxins that could pose a severe threat to plants and animals.[31] Final regulations to implement the May 2002 law were published in April 2005.[32]

These efforts to control access to dangerous pathogens came under harsh scrutiny in late 2008 after the FBI identified Bruce Ivins, a U.S. Army biodefense scientist, as the likely perpetrator behind the 2001 anthrax letters. This led

30. The law exempted clinical specimens (i.e., patient blood or tissue) being transferred for diagnostic and verification purposes and certain toxins and vaccine strains of select agents. Department of Health and Human Services, Centers for Disease Control and Prevention, "42 CFR Part 72: Additional Requirements for Facilities Transferring or Receiving Select Agents," *Federal Register* 61 (207) (October 24, 1996): 55190, https://www.gpo.gov/fdsys/pkg/FR-1996-10-24/pdf/96-27082.pdf.

31. *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, Pub. L. 107-188 (2002). The relevant sections of the conference report, H. Report 107–481, may be found in the *Congressional Record* 148 (66) (May 21, 2002): H2721–2724.

32. For the HHS regulations, see 42 CFR 73.12. For the USDA regulations, see 9 CFR 121.12 and 7 CFR 331.

to a variety of proposals for refining the select agent list, strengthening personnel reliability, and enhancing laboratory safety and security. In May 2009, for example, the National Science Advisory Board for Biosecurity (NSABB), which had been created in 2004 to advise the U.S. government on biosecurity issues, proposed reducing or stratifying the select agent list to focus on the agents of greatest concern. The NSABB also recommended more rigorous vetting of foreign nationals with access to such agents.[33] In November 2009, the Working Group on Strengthening the Biosecurity of the United States, which had been established by President George W. Bush to review security at select agent facilities, echoed the call for a reduced or stratified select agent list as well as better coordination of U.S. government inspections and better guidance on inventory management and recordkeeping. The working group also recommended identifying or establishing a federal entity to coordinate biosecurity oversight across all relevant U.S. government agencies.[34]

After entering office, President Barack Obama also created an interagency experts panel to provide advice on the select agent program and laboratory security. In November 2010, the Federal Experts Security Advisory Panel (FESAP) called for the removal of twenty-five agents and toxins from the select agent list and the creation of a separate list of eleven biological agents and toxins that posed the greatest risk, so-called Tier 1 agents. To strengthen personnel reliability, FESAP recommended modifying the security risk assessment process to better assess mental health, as well as providing guidance to facilities for conducting preaccess suitability and ongoing reliability assessments. Finally, to enhance physical security, FESAP called for the development of risk assessment guidance and cybersecurity standards.[35]

In October 2012, HHS and the Department of Agriculture (USDA) issued revised select agent regulations that reflected many of these recommendations. Three new viruses were added to the select agent list, and twenty-two other agents and toxins were removed; eleven of the remaining sixty-three select

33. National Science Advisory Board for Biosecurity, *Enhancing Personnel Reliability among Individuals with Access to Select Agents* (Washington, D.C.: NSABB, May 2009), http://osp.od.nih.gov/sites/default/files/resources/NSABB%20Final%20Report%20on%20PR%205-29-09.pdf.

34. The Working Group on Strengthening the Biosecurity of the United States was established pursuant to Executive Order 13486, of January 9, 2009. See "Executive Order 13486 of January 9, 2009: Strengthening Laboratory Biosecurity in the United States," *Federal Register* 74 (9) (January 14, 2009): 2289–2291, http://www.gpo.gov/fdsys/pkg/FR-2009-01-14/pdf/E9-818.pdf. For the working group's report, see *Report of the Working Group on Strengthening the Biosecurity of the United States* (Washington, D.C., 2009), http://www.phe.gov/Preparedness/legal/boards/biosecurity/Documents/biosecreportfinal102309.pdf.

35. "Executive Order 13546 of July 2, 2010: Optimizing the Security of Biological Select Agents and Toxins in the United States," *Federal Register* 75 (130) (July 8, 2010): 39, 439–442, http://www.gpo.gov/fdsys/pkg/FR-2010-07-08/pdf/2010-16864.pdf; and Federal Experts Security Advisory Panel, *Recommendations Concerning the Select Agent Program* (revised) (Washington, D.C., June 13, 2011), http://www.phe.gov/Preparedness/legal/boards/fesap/Documents/fesap-recommendations-101102.PDF. The FESAP report was originally released November 2, 2010.

agents and toxins were designated Tier 1 because they present "the greatest risk of deliberate misuse with the most significant potential for mass casualties or devastating effects to the economy, critical infrastructure, or public confidence."[36] The revised select agent rules also established new personnel and physical security requirements for facilities with Tier 1 agents, including requirements for preaccess assessments and on-going monitoring of personnel with access to Tier 1 pathogens and toxins and for bolstering the use of barriers and intrusion detection devices. New guidance documents on personnel reliability and physical security were released along with the revised regulations.[37] One important recommendation that the U.S. government did not implement was for the creation of a federal entity to coordinate biosecurity oversight across government agencies.

In December 2014, FESAP issued new recommendations on laboratory biosafety and biosecurity[38] in response to disclosures the previous summer of three other incidents involving select agents: the accidental exposure of some eighty-four CDC laboratory workers to live anthrax; CDC's shipment of a relatively benign bird flu (H9N2) that had been contaminated with the highly lethal H5N1 influenza virus; and the discovery of vials of smallpox and other infectious agents that had been left in an unsecured storage area in an NIH lab for more than fifty years.[39] To help prevent similar incidents in the future, FESAP recommended that HHS and USDA establish a review body to validate the policies and protocols being used at select agent research facilities to inactivate, sterilize, and decontaminate hazardous biological materials. They also called for greater transparency in government reporting about laboratory incidents involving select agents and for a federal review to determine how many U.S. high-containment laboratories are needed for research on select agents.

In 2014, the most recent year for which data are available, 316 facilities and some eleven thousand individuals were approved to work with select agents.[40] But limited information is available from the U.S. government about the compliance of these facilities and individuals with the select agent regulations, as the last U.S. government audits appear to have been done in 2006, when ten out of ten institutions subject to USDA regulations and eleven out of fifteen institutions subject to HHS regulations were found by their respective agen-

36. Department of Health and Human Services, Centers for Disease Control and Prevention, "42 CFR Part 73: Possession, Use, and Transfer of Select Agents and Toxins; Biennial Review," *Federal Register* 77 (194) (October 5, 2012): 61084, http://www.gpo.gov/fdsys/pkg/FR-2012-10-05/pdf/2012-24389.pdf.

37. For the full text of the select agent regulations, see ibid., 61084–61115.

38. Report of the Federal Experts Security Advisory Panel, December 2014, http://www.phe.gov/s3/Documents/fesap.pdf

39. Dina Fine Maron, "CDC Botched Handling of Deadly Flu Virus," *Scientific American*, July 11, 2014, http://www.scientificamerican.com/article/cdc-botched-handling-of-deadly-flu-virus/.

40. Lori J. Bane, Associate Director for Policy, CDC Division of Select Agents and Toxins, personal correspondence, November 14, 2014.

cies to be in violation of at least one aspect of the select agent rules.[41] A 2015 investigation by a U.S. newspaper found that since 2003, HHS and USDA have cited more than one hundred laboratories for serious safety and security lapses. Of the labs subject to HHS oversight, seventy-nine have been referred for potential enforcement action, including nineteen who have been fined over $2.4 million. Since 2008, thirty-three labs have agreed to participate in performance improvement programs after repeated failures to correct past biosafety and security problems or to comply with security requirements for working with the most dangerous select agents. For its part, USDA has conducted forty-eight investigations of laboratories subject to its oversight, and has levied fines of about $117,000.[42]

Even as controls on select agents were first being implemented, attention began to focus on the risk that advances in gene synthesis technology might make possible the creation of select agents de novo, without naturally occurring nucleic acids or pathogens. In a report in 2006, the NSABB pointed to the global availability of gene synthesis suppliers, equipment, and reagents, as well as the diversity of practitioners, some of whom, such as high school students or engineers, had little exposure to biosafety rules. As noted earlier, although some commercial suppliers of gene sequences had begun to screen customer orders voluntarily, suppliers were uncertain about what actually fell within U.S. select agent laws and regulations. In order to prevent synthetically derived sequences from evading the select agent rules, the NSABB recommended that the U.S. government develop a process for commercial suppliers to use to determine which sequences to screen for—select agent or otherwise—as well as standards and practices for how to screen, including record keeping. The NSABB also called for the development and implementation of universal standards and practices for screening sequences and, longer term, an effort to replace the existing list of specific select agents with a broader sequence-based system focused on the predicted properties of select agents.[43]

41. Department of Agriculture, Office of Inspector General Southeast Region, *Audit Report: Animal and Plant Health Inspection Service Evaluation of the Implementation of the Select Agent or Toxin Regulations Phase II*, Report no. 33601-3-AT (Washington, D.C.: Department of Agriculture, January 2006), http://www.usda.gov/oig/webdocs/33601-3-AT.pdf; and Department of Health and Human Services, Office of Inspector General, *Summary Report on Universities' Compliance with Select Agent Regulations*, A-04-05-02006 (Washington, D.C.: Department of Health and Human Services, June 2006), http://oig.hhs.gov/oas/reports/region4/40502006.pdf. A 2014 audit of over 4,000 facilities found 27 instances in which select agents had not been registered properly. But the audit focused only on inventory controls at U.S. government facilities. "FACT SHEET: Biosafety and Biosecurity in the United States," December 16, 2014, http://www.cdc.gov/about/pdf/lab-safety/external-usg-wide-fact-sheet_bsat-safety-stand-down-and-summary-table_final_12-16-2014.pdf.

42. Alison Young and Nick Penzenstadler, "Inside America's Secretive Biolabs," *USA Today*, May 28, 2015, http://www.usatoday.com/story/news/2015/05/28/biolabs-pathogens-location-incidents/26587505/.

43. National Science Advisory Board for Biosecurity, *Addressing Biosecurity Concerns Related to the Synthesis of Select Agents* (Washington, D.C.: NSABB, December 2006), http://osp.od.nih.gov/sites/default/files/resources/Final_NSABB_Report_on_Synthetic_Genomics.pdf.

In October 2010, nearly four years after the NSABB report and a year after the International Association Synthetic Biology and the International Gene Synthesis Consortium had issued their own proposals for sequence and customer screening, the U.S. government released its guidance for commercial gene synthesis suppliers. This guidance was weaker than the approaches recommended by the NSABB and by the gene synthesis industry because it was both voluntary and focused on screening customer orders only for sequences associated specifically with select agents. In addition to outlining steps for sequence and customer screening, the guidance also addressed record keeping and screening software.[44]

U.S. Measures Governing the Handling and Use of Biological Agents

U.S. efforts to govern the handling and use of biological agents date to the mid-1970s, when concerns about the potential risks of the new field of biotechnology led the National Institutes of Health (NIH) to create the Recombinant DNA Advisory Committee (RAC) to develop guidelines for the conduct of recombinant DNA (rDNA) research. The first *NIH Guidelines for Research Involving Recombinant DNA Molecules (NIH Guidelines)* classified agents into four risk groups based on their relative pathogenicity for healthy human adults and outlined the combination of laboratory practices, equipment, and facilities appropriate both for the agent and the proposed experiment. For rDNA research, this was supplemented by the use of biological barriers to limit the infectivity of a vector for specific hosts or to limit its dissemination and survival in the environment. Specific plant and animal pathogens also had special handling conditions. Research facilities were required to establish institutional biosafety committees (IBCs) to ensure that their rDNA work was done in accordance with the *NIH Guidelines*, which applied to all rDNA research conducted at institutions in the United States and abroad that received funds from NIH for such research. The guidelines were voluntary but included penalties for noncompliance, including the loss of NIH funds for rDNA research.[45]

In 1984, HHS published the first consolidated U.S. safety guidelines for laboratory activities involving biological agents. Like the *NIH Guidelines*, the HHS manual on *Biosafety in Microbiological and Biomedical Laboratories* (BMBL) categorizes agents into four classes or levels depending upon their degree of risk and describes the combination of laboratory practices, equipment, and facilities recommended to work safely with those agents. Following the adoption of the select agent program, the BMBL began to address laboratory biosecurity as well, providing guidance not only on risk assessment methodol-

44. Department of Health and Human Services, *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA* (Washington, D.C.: Department of Health and Human Services, October 2010), http://www.phe.gov/Preparedness/legal/guidance/syndna/Documents/syndna-guidance.pdf.

45. Department of Health and Human Services, National Institutes of Health, *NIH Guidelines for Research Involving Recombinant or Synthetic Nucleic Acid Molecules (NIH Guidelines)* (Washington, D.C.: Department of Health and Human Services, November 2013), http://osp.od.nih.gov/sites/default/files/NIH_Guidelines_0.pdf.

ogy but on physical security, personnel management, inventory controls, and other aspects of a laboratory biosecurity plan. As with its approach to biosafety, the BMBL's biosecurity guidance links the protection of biological agents and toxins to their identified risks. Although the BMBL represents voluntary guidelines, U.S. government contractors and grantees as well as facilities registered to work with select agents are required to follow the manual.[46]

Beginning in 1993, the U.S. Army published detailed guidance for Army personnel, contractors, and subcontractors engaged in biological research, development, test, and evaluation (RDT&E) activities under its biological defense program.[47] Shortly after the anthrax letters, the Army began to develop a biological surety program to strengthen the safety and security of dangerous pathogens and toxins at its facilities. This "biosurety" program, which was not implemented formally until 2008, was based on those the military already had developed for nuclear and chemical weapons and focused on laboratory safety, physical security, agent accountability, and personnel reliability.[48] Later that year, following the anthrax charges against Army biodefense scientist Ivins, the DOD Inter-Service Council for Biosecurity and Biosafety recommended upgrading background-check requirements, increasing supervisor review and control of after-hours access to labs, and improving control over select agent stocks at DOD facilities.[49] A Defense Science Board task force on biosafety and biosecurity further recommended improving the video monitoring of DOD labs and better coordination of laboratory inspections.[50]

U.S. government regulations also address other aspects of the handling of biological agents in an effort to prevent harm to human beings, animals, plants, and the environment. For example, under the Toxic Substances Control Act, the Environmental Protection Agency (EPA) regulates commercial research and development with new microorganisms and any other microorganisms the agency determines are for a significant new use.[51] Under USDA regulations,

46. Department of Health and Human Services, *Biosafety in Microbiological and Biomedical Laboratories*, 4th ed. (Washington, D.C.: U.S. Government Printing Office, 2009); and Frank Gottron and Dana A. Shea, *Oversight of High-Containment Biological Laboratories: Issues for Congress*, CRS Report for Congress, R40418 (Washington, D.C.: Congressional Research Service, May 2009), 8.

47. Department of the Army, "Biological Defense Safety Program, Technical Safety Requirements," Army Regulation 385-69, December 31, 1993, at 32 CFR 627.

48. Department of the Army, "Biological Surety," Army Regulation 50–1, July 28, 2008.

49. Government Accountability Office, *High Containment Laboratories: National Strategy for Oversight Is Needed*, GAO-09-574 (Washington, D.C.: GAO, September 2009), http://www.gao.gov/new.items/d09574.pdf.

50. Department of Defense, Defense Science Board, *Report of the Defense Science Board Task Force on Department of Defense Biological Safety and Security Program* (Washington, D.C.: Department of Defense, May 2009), http://www.acq.osd.mil/dsb/reports/ADA499977.pdf.

51. New microorganisms are defined as microorganisms "formed by the deliberate combination of genetic material originally isolated from organisms of different taxonomic genera." 15 USC 2604 and 40 CFR 725.3. See also *Fact Sheet—Microbial Products of Biotechnology: Final Regulations under the Toxic Substances Control Act* (n.d.).

any person wishing to import, move, or release genetically engineered plant pests must either provide notification to or obtain a permit from the USDA.[52]

Research Oversight

U.S. efforts to oversee consequential biological research have followed two distinct but parallel tracks. The first track involves the *NIH Guidelines*, which in addition to prescribing physical containment requirements for rDNA research also originally prohibited six types of rDNA experiments because of biosafety concerns.[53] In the late 1970s, these restrictions in the guidelines began to be loosened as concerns about the risks of biotechnology research diminished. By 1982 the research prohibitions in the original guidelines had been eliminated, and local IBCs and institutional review boards (IRBs; for overseeing human subject research) had replaced the RAC as the primary authority for reviewing and approving most rDNA research.[54] Serious questions, however, began to be raised about compliance with these local review requirements after a 2004 study of U.S.-based IBCs revealed that scores of U.S. biotechnology companies had no IBC registered with NIH and that many of the university and other IBCs that were registered either did not meet or issued blanket approvals rather than review each research project separately.[55]

By comparison, oversight of the rDNA experiments that remain subject to NIH approval under the *NIH Guidelines* has been made even stronger since 2001. Under the May 2002 bioterrorism bill, any rDNA experiment that must be approved by NIH also has to be approved by the secretary of HHS or the administrator of USDA's Animal and Plant Health Inspection Service if it involves agents or toxins on either department's select agent list. From January 2006 to December 2013, ninety-one of these so-called restricted experiments were proposed to HHS, of which thirty-one were approved. The remaining sixty experiments, all of which involved inserting drug-resistance traits into select agents, were not approved because they posed potentially serious risks to public health and safety. In recent years there have been four violations of the legal requirements governing HHS's oversight of restricted experiments, two of which resulted in civil penalties ranging from $40,000 to $1 million.[56]

52. 7 CFR 340.3 and 7 CFR 340.4.

53. Donald Fredrickson, *The Recombinant DNA Controversy, a Memoir: Science, Politics, and the Public Interest, 1974–1981* (Washington, D.C.: ASM Press, 2001), 39–40.

54. Epstein, "Controlling Biological Warfare Threats," 338; and Ronald M. Atlas, "Applicability of the NIH Recombinant DNA Advisory Committee Paradigm for Reducing the Threat of Bioterrorism" (draft paper prepared for the Controlling Dangerous Pathogens Project, April 2002), 3–8.

55. Sunshine Project, *Mandate for Failure: The State of Institutional Biosafety Committees in an Age of Biological Weapons Research* (Austin: Sunshine Project, October 2004).

56. Jacinta Smith, Denise Gangadharan, and Robbin Weyant, "Review of Restricted Experiment Requests, Division of Select Agents and Toxins, Centers for Disease Control and Prevention, 2006–2013," *Health Security* 13 (5) (2015): 307–316.

No comparable data on restricted experiment proposals or violations have been released by USDA.

In April 2010, the NSABB proposed expanding the *NIH Guidelines* to include synthetic biology, which seeks to create novel biological structures with predictable properties and functions, either by reengineering existing organisms or genomes or assembling nonliving biological components in novel ways. Governance of this evolving field, as the NSABB noted in a report at the time, is challenging because of the difficulty of predicting the biological characteristics of the new systems being created; the pace of developments and volume of information being produced; the diversity of disciplines involved, which includes the life sciences, engineering, chemistry, materials science, and computer modeling; and the variety of practitioners, not only university and high school students but also private sector and amateur scientists. Despite these challenges, the NSABB recommended establishing oversight arrangements for research with synthetic nucleic acids, including by explicitly adding synthetic nucleic acids to the *NIH Guidelines*.[57] NIH implemented the NSABB recommendation two years later, expanding the guidelines to include research with synthetic nucleic acid molecules even if rDNA techniques are not used.[58]

The second track of U.S. efforts to oversee biological research has focused on the security concerns raised by dual-use research. This began in the summer of 2001 when, spurred in part by the Australian mousepox experiment, the U.S. National Academy of Sciences convened an expert panel chaired by Massachusetts Institute of Technology professor Gerald Fink to examine the risks from dual-use biotechnology research. The Fink Committee, as it came to be called, issued its aptly titled report, *Biotechnology Research in an Age of Terrorism*, in October 2003. The report emphasized that dual-use biotechnology research has the capacity "to cause disruption or harm, potentially on a catastrophic scale"; it also pointed out that U.S. and international measures governing such research do not address this security threat, in that they focus largely on biosafety and nonproliferation.

To help fill this gap, the Fink Committee proposed adding seven types of what it called "experiments of concern" to the research oversight process already in place under the *NIH Guidelines*. Specifically, it called for local IBC review followed, if necessary, by further review by the RAC or the NIH director, of any experiment that would

- demonstrate how to render a vaccine ineffective;
- confer resistance to antibiotic or antiviral agents;

57. National Science Advisory Board for Biosecurity, *Addressing Biosecurity Concerns Related to Synthetic Biology* (Washington, D.C.: NSABB, April 2010), http://osp.od.nih.gov/sites/default/files/resources/NSABB%20SynBio%20DRAFT%20Report-FINAL%20%282%29_6-7-10.pdf.

58. For information on the *NIH Guidelines*, see National Institutes of Health, "Biosafety: NIH Guidelines," n.d., http://osp.od.nih.gov/office-biotechnology-activities/biosafety/nih-guidelines.

- enhance the virulence of a pathogen or render a nonpathogen virulent;
- increase the transmissibility of a pathogen;
- alter the host range of a pathogen;
- enable evasion of diagnosis or detection methods; or
- enable weaponization of a biological agent or toxin.

The committee noted that these seven types of experiments represented current dangers but that additional types of experiments would need to be included in the future to address other potential threats. The committee also acknowledged that although oversight would initially apply only to research at facilities that were subject to the NIH guidelines, eventually *all* relevant research, including in private-sector and non-NIH government facilities, should be included in the oversight process. To help address these issues, the Fink Committee proposed the establishment of a national science advisory board for biodefense within HHS.[59] The creation of the NSABB in March 2004 was a direct result of the Fink Committee's recommendations.

In June 2007, after more than three years of deliberations, the NSABB released a proposed framework for oversight of dual-use research. The NSABB proposal differed from the Fink Committee's approach in a number of important respects. First, the NSABB focused on dual-use research of concern (DURC), a subset of dual-use research. Second, rather than have IBCs make the initial determination of whether research was of potential concern, the NSABB proposed that researchers do this themselves. Third, the NSABB proposed a single criterion for researchers to use to determine if their work met the definition of DURC—whether, based on current understanding, the research can be "*reasonably anticipated* to provide knowledge, products, or technologies that *could* be directly misapplied by others to pose a threat to public health and safety, agricultural crops and other plants, animals, the environment, or material."[60] Finally, recognizing that determining the applicability of this criterion would be a "subjective and challenging task," the NSABB outlined seven broad categories of experimental effects (similar to the Fink Committee's experiments of concern) that, if generated by the proposed research, *might* mean that it met the DURC criterion and thus required further institutional review or oversight by an IBC or other expert review committee. [61]

Although the NSABB initially recommended applying its oversight framework to federally funded research only, it later shifted position, arguing in its

59. National Research Council, Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism* (Washington, D.C.: National Academies Press, 2003), http://www.nap.edu/openbook.php?record_id=10827.

60. National Science Advisory Board for Biosecurity, *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information* (Washington, D.C.: NSABB, 2007), http://osp.od.nih.gov/sites/default/files/resources/Framework%20for%20transmittal%20duplex%209-10-07.pdf; emphasis added.

61. Ibid.

April 2010 synthetic biology report that dual-use oversight should be uniform and comprehensive, extending beyond the life sciences and academia to include other practitioners, including in the private sector.[62] The NSABB was silent, however, on the issue of classified biodefense research, which was explicitly outside the scope of its responsibilities. This was especially unfortunate, given that the biodefense research program then being developed by DHS for its new National Biodefense Analysis and Countermeasures Center fell squarely within the Fink Committee's seven experiments of concern.[63]

Even before the NSABB oversight framework was released publicly in June 2007, CDC put in place a DURC review process for its own research activities, known as *intramural* research, based on the NSABB's recommendations.[64] NIH did the same in 2008.[65] In presentations at a biosafety conference in 2010, NIH researchers reported that a retrospective review of NIH intramural research projects approved between 2004 and 2009 showed that only a small subset of biomedical research raised potential dual-use concerns in their *initial* screening (101 of 3,444 in one study and 12 of 734 in another) and that further expert review determined that only two projects actually met the definition of DURC. The NIH review also concluded that dual-use review was "easily incorporated" into existing IBC review processes and resulted in "no additional cost" and "no adverse effects" on research progress.[66] A CDC review of manuscripts from its intramural research program found that from 2007 to 2010, only eight manuscripts raised DURC questions, out of an annual publication rate of approximately 3,000 articles. After additional review, all eight manuscripts were published substantively "as is."[67] Neither NIH nor CDC has released information since 2010 on the impact of their respective DURC review processes.

Despite CDC and NIH's efforts to review their own intramural research, nearly five years passed before a broader policy for *U.S. government DURC* was announced. The release of this policy in March 2012 was a direct result of controversy over two external or *extramural* research projects on the H5N1

62. NSABB, *Addressing Biosecurity Concerns Related to Synthetic Biology.*

63. Milton Leitenberg, James Leonard, and Richard Spertzel, "Biodefense Crossing the Line," *Politics and the Life Sciences* 22 (2) (2003): 2–3, http://www.politicsandthelifesciences.org/Contents/Contents-2003-9/PLS2003-9-22-02-0002.pdf.

64. Centers for Disease Control and Prevention, *Oversight and Clearance of Dual-Use Research of Concern*, CDC-SM-2007-01 (Atlanta, GA: CDC, March 23, 2007).

65. Megan C. Morgan, "Evaluation of a First-Tier Screening Program for Dual-Use Research of Concern" (presentation at the 53rd Annual Biological Safety Conference, Denver, October 5, 2010), http://www.absaconference.org/pdf53/Session11-Morgan.pdf.

66. Morgan, "Evaluation of a First-Tier Screening Program for Dual-Use Research of Concern"; and Molly S. Stitt-Fischer, "The National Institutes of Health Dual Use Screening Program: A Proposed Quality Control Model" (presentation at the 53rd Annual Biological Safety Conference, Denver, October 5, 2010), http://www.absaconference.org/pdf53/Session11-Stitt-Fischer.pdf.

67. Mary D. Ari, PhD, "CDC's Implementation of Dual-Use Research of Concern (DURC) Oversight" (presentation at the Council of Science Editors Annual Meeting, Seattle, May 20, 2012), http://www.resourcenter.net/images/cse/files/2012/annmtg/handouts/03_ari_3.pdf.

influenza virus, which had been funded by NIH without considering dual-use concerns. The new policy, which applied only to unclassified life sciences research funded or conducted by the U.S. government, drew heavily on both the Fink Committee's original experiments of concern and the NSABB's single, proposed criterion for assessing research. But it also narrowed the NSABB approach by adding a requirement that the research also had to involve one of fifteen specific agents or toxins from the select agent list. Agencies were ordered to review their intramural and extramural research projects to determine whether they involved DURC and, if so, to conduct risk-benefit assessments, develop risk mitigation plans, and provide periodic reports on the projects.[68]

Concern over the H5N1 influenza research projects (one of which had been conducted by Dutch scientists)—including questions about the scientific value of the research, the biosafety conditions under which the projects were undertaken, and the dissemination of the results—continued to draw attention to the adequacy of U.S. oversight policies for dual-use research. But instead of examining the effectiveness of its approach more broadly, the U.S. government reacted in a piecemeal way, outlining first, in February 2013, a complicated and lengthy process by which HHS would make future *funding* decisions on certain highly pathogenic avian influenza (HPAI) research proposals. These studies were called "gain of function" (GOF) research, because they involved modifying already dangerous pathogens in order to increase their transmissibility or pathogenicity or to alter their host range.[69] Six months later, HHS extended the H5N1 funding review process to proposed experiments with the H7N9 influenza virus after twenty-two scientists published letters in *Nature* and *Science* seeking support for conducting GOF experiments with H7N9, which had emerged earlier in the year in China and was believed to pose a potential pandemic risk.[70]

Despite, or perhaps because of these piecemeal steps, the controversy over GOF research did not end. In early 2014, other work to create new virus strains similar to the 1918 pandemic virus and to enable the H1N1 virus to evade the human immune system produced an outcry among scientists that spread quickly to the mainstream press in the United States and abroad.[71] Concerns

68. *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern* (Washington, D.C., March 2012), http://www.phe.gov/s3/dualuse/documents/us-policy-durc-032812.pdf.

69. Department of Health and Human Services, *A Framework for Guiding U.S. Department of Health and Human Services Funding Decisions about Research Proposals with the Potential for Generating Highly Pathogenic Avian Influenza H5N1 Viruses That Are Transmissible among Mammals by Respiratory Droplets* (Washington, D.C.: HHS, February 2013), http://www.phe.gov/s3/dualuse/Documents/funding-hpai-h5n1.pdf.

70. David Malakoff, "Critics Skeptical as Flu Scientists Argue for Controversial H7N9 Studies," *Science* 341 (6146) (August 9, 2013): 601; and Harold Jaffe, Amy P. Patterson, and Nicole Lurie, "Extra Oversight for H7N9 Experiments," *Science* 341 (6147) (August 16, 2013): 713–714.

71. See, for example, "Scientists Condemn 'Crazy, Dangerous' Creation of Deadly Airborne Flu Virus," *Guardian*, June 11, 2014; and Steve Connor, "Exclusive: Controversial US Scientist Creates Deadly New Flu Strain for Pandemic Research," *Independent*, July 1, 2014.

about the safety and security of research with highly dangerous pathogens were reinforced at the same time by the reports that had come to light regarding the mishandling of anthrax, the H5N1 influenza virus, and smallpox at government research facilities.

In July 2014, a call to curtail experiments involving the creation of potential pandemic pathogens pending further analysis and the convening of a meeting to discuss such work was issued by eighteen leading scientists and quickly endorsed by nearly three hundred other U.S. and foreign scientists and policy experts. Other scientists more positively disposed toward GOF research also endorsed the meeting idea.[72] In October 2014, the White House Office of Science and Technology Policy responded, announcing that the U.S. government would undertake a deliberative process on GOF experiments with help from the NSABB and the National Research Council of the National Academies in order to develop a new U.S. policy on the conduct and funding of such research. The White House also announced a funding pause on new GOF studies involving influenza, severe acute respiratory syndrome (SARS), and Middle East respiratory syndrome (MERS) viruses and encouraged those already conducting such work to pause voluntarily until a new policy was in place.[73] (The White House subsequently lifted the pause on five MERS and two influenza studies.[74])

Over the next eighteen months, the NSABB held five meetings and commissioned both a risk-benefit assessment study and an analysis of the ethical issues surrounding GOF research.[75] The former, a $1 million, one-thousand-page contractor effort, was highly criticized by opponents of GOF research on technical and analytical grounds, including the study's failure to calculate the probability of an enhanced pathogen escaping the laboratory, a key variable in the calculation of pandemic risk. The study was also criticized for bias, in that 80 percent of the scientists interviewed about the benefits of GOF research were either scientists who conducted such research or representatives of agencies

72. "Cambridge Working Group Consensus Statement on the Creation of Potential Pandemic Pathogens (PPPs)," July 14, 2014, http://www.cambridgeworkinggroup.org/; and "Scientists for Science," *Virology Blog*, July 28, 2014, http://www.virology.ws/2014/07/28/scientists-for-science/.

73. Department of Health and Human Services, *U.S. Government Gain-of-Function Deliberative Process and Research Funding Pause on Selected Gain-of-Function Research Involving Influenza, MERS and SARS Viruses: Frequently Asked Questions* (Washington, D.C.: HHS, November 2014), http://www.phe.gov/s3/dualuse/Documents/gof-qanda.pdf.

74. Nell Greenfieldboyce, "NIH Allows Restart of MERS Research That Had Been Questioned," *Shots: Health News from NPR*, December 18, 2014, at http://www.npr.org/sections/health-shots/2014/12/18/371686933/nih-allows-restart-of-mers-research-that-was-deemed-too-risky.

75. Joseph Kanabrocki, "NSABB Working Group Report: Preliminary Findings and Draft Recommendations," PowerPoint presentation for National Science Advisory Board for Biosecurity meeting January 7–8, 2016, http://osp.od.nih.gov/sites/default/files/NSABB%20Working%20Group%20-%20Preliminary%20Findings%20and%20Draft%20Recommendations.pdf.

who funded it.[76] The ethical study, by comparison, provided a comprehensive, balanced discussion of the various ethical and decision-making frameworks of potential relevance to evaluating GOF proposals. Of particular importance was the study's suggestion that a federal advisory body like the NSABB might play a role in reviewing GOF research.[77]

The NSABB also prepared a draft working paper outlining its initial thoughts on a conceptual approach for reviewing proposed GOF studies. As in its earlier work on dual-use research, the NSABB recommended focusing GOF oversight on research that posed the greatest risk, or what it called GOF studies of concern. The working paper also recommended that oversight for these studies should be incorporated into existing policy frameworks (for example, the NIH Guidelines and the oversight policies for DURC), although it recognized that additional oversight might be required in some cases.[78] The National Research Council contributed to the NSABB's work by holding two symposiums to elicit input from the scientific community and the public. The first symposium focused on scientific and technical questions related to the conduct of risk-benefit assessments of GOF research. The second symposium examined possible oversight policies, including the recommendations in the draft NSABB working paper.[79]

In the coming months, the NSABB is expected to refine and elaborate its proposed recommendations and, ultimately, submit a final report to the federal government for consideration. But whether the policy that emerges from the U.S. deliberative process is effective will depend not only on the details of the oversight arrangements but also on the policy's scope: whether it applies only to U.S. government funded research, as currently planned, or is used to review all relevant research in the United States and, eventually, other countries.

In parallel with the 2014 announcement of the GOF deliberative process, the U.S. government also finally released in September 2014, nearly seven years after the NSABB oversight proposal, a new policy on the responsibilities of *research institutions* involved in dual-use research. Like the 2012 policy for

76. Gryphon Scientific, "Risk and Benefit Analysis of Gain of Function Research," Draft Final Report, December 2015, http://osp.od.nih.gov/sites/default/files/Risk%20and%20Benefit%20Analysis%20of%20Gain%20of%20Function%20Research%20-%20Draft%20Final%20Report.pdf. For public comments on the report, see http://dels.nas.edu/resources/static-assets/bls/agenda/Compiled%20Public%20Comments%20to%20NAS%20and%20NSABB%20-%20ALL%20COMMENTS.pdf.

77. Michael J. Selgelid, "Gain of Function Research: Ethical Analysis," White Paper, n.d., http://osp.od.nih.gov/sites/default/files/Gain-of-Function%20Research%20Ethical%20Analysis%20White%20Paper%20by%20Michael%20Selgelid_0.pdf.

78. National Science Advisory Board for Biosecurity, "Working Paper Prepared by the NSABB Working Group on Evaluating the Risks and Benefits of Gain-of-Function Studies to Formulate Policy Recommendations," Deliberative Draft, December 23, 2015, http://osp.od.nih.gov/sites/default/files/NSABB%20WG%20Working%20Paper%20on%20Gain-of-Function%20Studies%2012-23-2015_0.pdf.

79. For the report from the first symposium, see http://dels.nas.edu/Workshop-Summary/Potential-Risks-Benefits-Gain/21666?bname=bls; for information on the second symposium, see http://dels.nas.edu/Upcoming-Event/Gain-Function-Research-Second/AUTO-9-61-70-Q.

U.S. government DURC, this new policy applies only to unclassified research involving one or more of fifteen specific select agents and toxins. But it also is somewhat broader than the 2012 policy in that it covers relevant research at any institution (e.g., government, academic, or private) that receives federal funding for life sciences research, even if the U.S. government is not funding the project in question. However, both research at institutions that do not receive federal funds for life sciences research and classified research (including for biodefense) remain outside the scope of U.S. DURC oversight requirements.

Under the new U.S. policy, the DURC review process begins only after a research project has secured funding. The primary investigator (PI) is expected to initiate the DURC review and to work with an institutional review entity (IRE), such as an IBC, to conduct a risk-benefit assessment and, if appropriate, to develop a draft risk mitigation plan. The IRE is responsible for making the final determination of whether the research is DURC, for ensuring that an appropriate risk mitigation plan is in place, and for reviewing both the plan and the research on an annual basis. The institution where the DURC is to be carried out is responsible for notifying the appropriate U.S. government agency of the DURC determination and for submitting the draft risk mitigation plan for final approval. Although the policy is not legally based, failure to comply could lead to the loss of existing or future U.S. government research funds.[80]

Current State of Governance in Other Countries

As in the United States, other countries also have adopted measures aimed at preventing the spread of biological weapons capabilities or ensuring the safety and security of work involving dangerous biological materials (see Table 4). For example, EU members have enacted national legislation to implement the BWC's prohibitions against biological weapons development and acquisition. Since 1994, EU member states also have approved various regulations and directives designed to control exports of dual-use items, including those related to biological weapons. These regulations and directives are binding on every EU country. Under European Council regulation (EC) 3381/94, member states must require a license for exports outside the EU of biological materials, equipment and technical information. Consistent with AG controls, the regulation also includes a "no-undercut" policy as well as catch-all controls requiring the licensing of any nonlisted dual-use items that pose a proliferation risk. Biological agents adapted for use in war and equipment specifically designed for biological weapons purposes are controlled by EU members under the EU's list of common military goods, which is based on the munitions list of the Wassenaar Arrangement, the multilateral export control regime that succeeded the Cold

80. *United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern* (Washington, D.C., September 24, 2014), http://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf.

War–era Coordinating Committee for Multilateral Export Controls, known as CoCOM.[81]

Because of concerns about the safety of genetic modification techniques generally and genetically modified foods specifically, EU member states also have enacted directives on the safe handling of genetically modified organisms (GMOs). For example, under European Council Directive 90/219/EEC, facilities must notify their relevant government authority before using GMOs for the first time. The notification must include a description of the proposed work, an assessment of the risks to human health and the environment, and other information depending on the characteristics of the organism and level of containment required. Activities requiring Level 3 containment or above may not proceed without prior government approval.[82] Under European Council Directive 90/220/EEC, before deliberately releasing a GMO into the environment, a manufacturer or importer must submit a notification to the government containing a full assessment of the risks to human health, animal health, and the environment of the proposed release, as well as detailed information on the GMO, the release plans and receiving environment, and monitoring and control arrangements. Final authority for approving the release resides with the European Commission.[83] Violators may be subject to penalties within EU member states.

81. (EC) 3381/94 established the general principles while Annex I of 94/942/CFSP contained the original control lists. These were later combined in (EC) 1334/2000. The most recent version of which is (EU) 388/2012. See "Report to Parliament and the Council on the Implementation of Council Regulation (EC) No 1334/2000 Setting Up a Community Regime for the Control of Exports of Dual-Use Items and Technology, October 2000 to May 2004," 20 September 2004, http://trade.ec.europa.eu/doclib/docs/2004/september/tradoc_118993.pdf; and German Ethics Council, *Biosecurity—Freedom and Responsibility of Research* (Berlin: Deutscher Ethikrat, May 2014), http://www.ethikrat.org/files/opinion-biosecurity.pdf. For the EU munitions list, see "Common Military List of the European Union," *Official Journal of the European Union*, C 90 (March 27, 2013): 1–37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:090:0001:0037:EN:PDF.

82. "Council Directive of 23 April 1990 on the Contained Use of Genetically Modified Micro-organisms (90/219/EEC)," *Official Journal of the European Union*, L 117 (May 8, 1990): 1–14, http://www.biosafety.be/GB/Dir.Eur.GB/Cont.Use/90.219/TC.html. For the amended version, 2009/41/EC, see "Directive 2009/41/EC of the European Parliament and of the Council of 6 May 2009 on the Contained Use of Genetically Modified Micro-organisms (Recast)," *Official Journal of the European Union*, L 125 (May 21, 2009): 75–97, http://www.biosafety.be/PDF/2009_41_EN.pdf?REQUEST=Seek-Deliver&COLLECTION=oj&SERVICE=eurlex&LANGUAGE=en&DOCID=2001l073p0032. The EU's "Level 3" corresponds to biosafety level (BSL) 3 in the United States. The biosafety level refers to the level of physical containment required for work with biological materials in a laboratory facility. The levels are designated in ascending order from BSL-1 (the lowest) to BSL-4 (the highest), with each level building on the previous level's requirements for laboratory practices, safety equipment, and facility design.

83. "Council Directive of 23 April 1990 on the Deliberate Release into the Environment of Genetically Modified Organisms (90/220/EEC)," *Official Journal of the European Union*, L 117 (May 8, 1990): 15–27, http://www.biosafety.be/GB/Dir.Eur.GB/Del.Rel./90.220/TC.html. For the amended version, 2001/18/EC, see "Directive 2001/18/EC of the European Parliament and of the Council of 12 March 2001on the Deliberate Release into the Environment of Genetically Modified Organisms and Repealing Council Directive 90/220/EEC," *Official Journal of the European Union*, L 106 (April 17, 2001): 1–39, http://eur-lex.europa.eu/resource.html?uri=cellar:303dd4fa-07a8-4d20-86a8-0baaf0518d22.0004.02/DOC_1&format=PDF.

Table 4: Biological Technology Governance in Other Countries

Measure	Date	Country	Purpose	Comments
90/219 EEC	1990	EU members	Control contained use of GMOs; prenotify first use; prior approval for Level 3 work or above	Legally binding; continues to be revised
90/220 EEC	1990	EU members	Control release of GMOs; prenotify release; prior approval by EC	Legally binding; penalties for violations; continues to be revised
3381/94 EC	1994	EU members	Control exports of biological agents, toxins, related equipment to proliferant countries	Legally binding; follows Australia Group control lists; continues to be revised
Anti-Terrorism, Crime and Security Act	2001 2007	UK	Control access to human pathogens and toxins: notification and security requirements; background checks	Legally binding Added plant pathogens
Code of Conduct for Biosecurity	2007	Netherlands	Guidance for screening dual-use research & facility access	Not legally binding; proposed by KNAW at government request; subsequently determined not sufficient
Act on Securing Biological Substances, Delivery Systems, Related Materials Executive Order	2008 2009	Denmark	Control access to biological substances, delivery systems and related materials; oversight of dual-use research Requires licensing, vulnerability assessment, security plan, access controls, and recordkeeping	Legally binding; penalties for violations; dual-use review process relegated to subsidiary documents
Laboratory Biorisk Management Standard	2008	EU	Guidance for handling biological materials in labs and other facilities	Politically binding; little information on national implementation
Regulation of Research into Biological Disease Agents Act	2008	Israel	Control access to biological agents by facility authorization; oversight of dual-use research by institutional committees	Legally binding; national-level council assists implementation
Human Pathogens and Toxin Act	2009	Canada	Strengthen controls on access to human pathogens and toxins by facility licensing, security clearances for high-risk agents, and inspections	Legally binding
Chemical, Biological, Radiological, Nuclear Action Plan	2009 2011	EU members	Prevent unauthorized access to materials of concern Agree on common control lists	Politically binding; no information on implementation

Members of the EU also have taken steps to prevent terrorists or other nonstate actors from acquiring or using biological agents, although few of these measures are legally binding. One exception is the Anti-Terrorism, Crime and Security Act of 2001 (ATCSA), which was adopted by the UK after September 11 and the anthrax letters to control access to biological agents that could be used against human beings, including genetic elements and genetically modified organisms associated with those agents. Under the ATCSA, facilities that possess or plan to possess these agents are required to notify the government and comply with any reasonable security enhancements imposed after an inspection of the site. They also are required to comply with official requests for information about security at their facility and about persons who have or are proposed to have access to controlled pathogens. Background checks may be conducted by the government, which may also deny individuals access to controlled pathogens or facilities where they are located. In 2007, following a foot-and-mouth disease outbreak in Surrey, the ATCSA was extended to include animal pathogens as well.[84]

In 2009, EU members adopted an action plan that, among other things, seeks to block unauthorized access to biological and other materials of concern. In 2011, members agreed on a common control list for each type of material, including a list of high-risk biological agents. EU members also agreed to implement the European Committee for Standardization's Laboratory Biorisk Management Standard, which provides guidance for handling biological materials in laboratories and other facilities based on WHO biosafety and biosecurity guidelines.[85] EU member states have released relatively little information about their implementation of these measures, which are politically but not legally binding.

Outside of the EU, Canada has strengthened its domestic controls on access to biological materials, which originally applied only to human pathogens and toxins that were being imported into the country. In 2009, the Canadian Parliament adopted the Human Pathogens and Toxin Act, which revised Canadian law to include all risk group 2, 3, and 4 human pathogens and toxins, natural

84. Statutory Instrument 2001 (no. 4019), *Anti-terrorism, Crime and Security Act 2001*, http://www.opbw.org/nat_imp/leg_reg/uk/ATCS.pdf. The 2007 revisions are described in "Pathogens and Toxins Guidance ATCSA 2001 Schedule 5 Order 2007 Notes (SI 2007/929)" (n.d.), http://www.cf.ac.uk/osheu/resources/Schedule%205%20pathogens%20and%20toxins%20list%20and%20guidance.pdf.

85. Commission of the European Communities, "On Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union—an EU CBRN Action Plan," COM(2009) 273 final, June 24, 2009, http://www.bureaubiosecurity.nl/dsresource?type=pdf&disposition=inline&objectid=rivmp:243738&versionid=&subobjectname; European Commission, "Progress Report on the Implementation of the EU CBRN Action Plan, May 2012," n.d., http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/securing-dangerous-material/docs/eu_cbrn_action_plan_progress_report_en.pdf; and European Committee for Standardization, *Laboratory Biorisk Management Standard*, CWA 15793:2008 (Brussels: European Committee for Standardization, February 2008), http://www.absa.org/pdf/CWA15793_Feb2008.pdf.

or synthetic, whether imported or acquired domestically.[86] Under recent implementing regulations, no person may possess, produce, store, transfer, release, or dispose of high-risk pathogens or toxins without first obtaining a government license. Before a license is issued, facilities are required to designate a biosafety officer, and facilities conducting scientific research are required to submit information on their biosafety and biosecurity procedures. The regulations also require that any person entering a facility area handling so-called security sensitive biological agents (a subset of risk group 3 and 4 human pathogens) must have a security clearance or be accompanied by someone with a clearance. Compliance monitoring through inspections, as well as enforcement actions, are also authorized under the law and regulations.[87]

Progress in strengthening oversight of dual-use life sciences research has been more limited, with few countries outside the United States having adopted research oversight policies. One that has is Denmark, which in June 2008 passed an Act on Securing Specific Biological Substances, Delivery Systems and Related Materials. Under the Danish law, dual-use research that can be used directly for the development of biological weapons or for offensive purposes is considered a type of technology and thus a "related material." The law applies to all entities, public or private, military or civilian, that handle, use, or store controlled items and thus combines in a more robust way the U.S. laws on select agents and U.S. policies on DURC.[88]

To ensure prompt implementation of the Danish biosecurity law as well as the flexibility to respond to future technological developments, both the lists of controlled items and the basic requirements were included in a separate executive order, which was adopted in 2009. Under the executive order, any entity that possesses or plans to possess a controlled item must obtain a license from the Danish biosecurity agency, known as the Center for Biosecurity and Biopreparedness (CBB). Such entities must prepare a vulnerability assessment and security plan for their site and appoint a biosafety officer to keep records of all individuals given access to controlled biological materials. Once licensed, they must maintain an inventory of all controlled items and submit to inspec-

86. "Risk group" refers to the classification of a biological agent based on its ability to cause disease. The risk groups are designated in ascending order from risk group 1, for agents that pose no or low risk, to risk group 4, for agents that pose the greatest risk.

87. "Human Pathogens and Toxin Regulations," *Canada Gazette* 148 (25) (June 21, 2014), http://www.gazette.gc.ca/rp-pr/p1/2014/2014-06-21/html/reg2-eng.php.

88. For a detailed discussion of the Danish approach, see Centre for Biosecurity and Biopreparedness, *An Efficient and Practical Approach to Biosecurity* (Copenhagen: CBB, 2015), https://www.biosikring.dk/fileadmin/user_upload/PDF_FILER/Biosecurity_book/An_efficient_and_Practical_approach_to_Biosecurity_web1.pdf.

tions by Danish authorities. Violations may result in fines, imprisonment, or criminal penalties.[89]

Because the 2009 executive order could not address every implementation detail, other CBB documents provide additional guidance, including on the process for evaluating research proposals for dual-use concerns. Scientists are responsible for conducting the initial screening of their research to determine whether it has dual-use potential, using a CBB questionnaire. If one or more of eleven possible research outcomes applies, the scientist must contact CBB so the agency can decide how possible risks should be addressed and whether a license or other form of regulation, such as restrictions on participation in the research or on its publication, is required.[90]

In November 2008, Israel adopted similar biosecurity legislation in response to a report by the Steering Committee on Biotechnological Research in an Age of Terrorism (COBRAT), a special committee created by the Israeli Academy of Sciences and Humanities and the Israeli National Security Council. Although modeled on the U.S. Fink Committee, COBRAT went much further than its American counterpart, recommending mandatory research oversight in all facilities, including government laboratories, as well as controls on dangerous biological agents.[91]

Under Israel's 2008 Regulation of Research into Biological Disease Agents Act, the Ministry of Health must authorize any institution or laboratory that possesses, conducts research on, or works with certain listed biological agents. Such institutions and laboratories are required to establish an institutional committee of scientists, security experts, and safety personnel to review research proposals for biosafety and biosecurity, including dual-use concerns. The law also provides for the creation of an interdisciplinary council to advise the Ministry of Health on the formulation and implementation of the necessary operating rules and regulations, including those governing the list of controlled agents, the proceedings of the institutional committees, and related issues.[92]

89. Danish Ministry of Health and Prevention, "Act on Securing Specific Biological Substances, Delivery Systems and Related Materials," ACT no. 474, June 17, 2008, https://www.biosikring.dk/fileadmin/user_upload/PDF_FILER/Biosikringsdokumenter/ACTNo474of17_June2008.pdf; and Danish Ministry of Health and Prevention, "Executive Order on Securing Specific Biological Substances, Delivery Systems and Related Materials," EO no. 981, October 15, 2009, https://www.biosikring.dk/499/.

90. Centre for Biosecurity and Biopreparedness, *An Efficient and Practical Approach to Biosecurity*, 115–16, 239–43; and Centre for Biosecurity and Biopreparedness, "Questionnaire about Dual Use Research of Concern for Companies, Project Managers, Etc.," August 18, 2015, https://www.biosikring.dk/fileadmin/user_upload/PDF_FILER/UK_forms_and_guides/Questionnaire_about_dual-use_research_of_concern.pdf.

91. Steering Committee on Issues in Biotechnological Research in an Age of Terrorism, *Biotechnology Research in an Age of Terrorism* (Jerusalem: Israel Academy of Sciences and Humanities and Israel National Security Council, 2008).

92. David Friedman, "Israel," in *Education and Ethics in the Life Sciences: Strengthening the Prohibition of Biological Weapons*, ed. Brian Rappert (Canberra: Australian National University Press, 2010), esp. 82–85, http://press.anu.edu.au?p=51221.

Recommendations also have been made in two other countries for research oversight policies, but as of early 2016 these have yet to be adopted. The first is the Netherlands, where in 2007 a biosecurity working group established by the Royal Netherlands Academy of Arts and Sciences (KNAW) proposed a code of conduct to prevent life sciences research from contributing to activities prohibited under the BWC or to any other misuse of biological agents or toxins. The KNAW *Code of Conduct for Biosecurity* outlines rules related to a number of issues, including screening for dual-use research as well as access to facilities involved in such work.[93] However, following the 2011 controversy over U.S. and Dutch research with the H5N1 virus, a separate KNAW biosecurity committee concluded that the code was not sufficient for addressing dual-use concerns and recommended the creation of an independent Biosecurity Advisory Committee for Research in the Life Sciences to advise researchers and institutions on relevant research proposals, including the conduct of the research and possible publications restrictions. The Dutch government has not responded to the biosecurity committee's report, although it has organized biosecurity workshops and published an online biosecurity questionnaire for use by those working with dangerous pathogens.[94]

The second country is Germany, where in 2014 the German Ethics Council released a report with two key research oversight recommendations. The first was to establish a national German code of conduct for responsible research to sensitize researchers and others to the risk of misuse and to define what constitutes responsible conduct. The council emphasized that the code should apply to all public and private facilities doing relevant research and should obligate researchers, after suitable training, to screen and monitor their own research for DURC. The council also recommended the adoption of legislation providing a legal definition of dual-use research of concern, establishing a national-level dual-use research interdisciplinary commission with the authority to vote on research projects, and requiring researchers to consult with the commission prior to and during the conduct of their research. To give its recommendations greater force, the council proposed that German funding bodies fund proposals only from researchers who comply with the code of conduct and have received a positive vote by the dual-use research commission. The council also proposed that the German government take the lead in trying to secure adoption of a similar dual-use research policy within the EU and of the code and definition of dual-use research of concern on a global level.[95] The German government has not responded to the Ethics Council report.

93. Royal Netherlands Academy of Arts and Sciences (KNAW), Biosecurity Working Group, *A Code of Conduct for Biosecurity* (Amsterdam: KNAW, 2008).

94. As described in German Ethics Council, *Biosecurity—Freedom and Responsibility of Research* (Berlin: German Ethics Council, 2014), http://www.ethikrat.org/files/opinion-biosecurity.pdf. Copies of the KNAW reports are available at https://www.knaw.nl/en/news/publications/improving-biosecurity.

95. German Ethics Council, *Biosecurity—Freedom and Responsibility of Research*, http://www.ethikrat.org/files/opinion-biosecurity.pdf.

Other Measures for Managing Biological Technology

While many proposals have been made over the last decade and a half for managing the risks from biological technology, two types warrant particular attention. The first, scientific codes, have received strong support from across the scientific community. The second, restrictions on the dissemination of sensitive dual-use research information, have elicited the opposite reaction, notwithstanding periodic debates over the need for a mechanism to that effect.

Codes for Scientists

Since the collapse of the BWC protocol negotiations, significant attention has focused on the utility of scientific codes in helping address dual-use concerns. Much of this discussion has focused on ethical codes, which describe personal and professional standards; or on codes of conduct, which provide guidelines on appropriate behavior. Little attention, however, has been given to codes of practice, which outline enforceable procedures and rules.[96]

At the suggestion of the United States, codes of conduct were a major topic of discussion in the BWC intersessional meetings in 2005. One important nongovernmental participant was the InterAcademy Panel (IAP), a global network of science academies from around the world. The IAP proposed five principles to guide the development of codes of conduct: (1) awareness of dual-use risks; (2) safe and secure laboratory practices; (3) education and information about dual-use laws, regulations, and policies; (4) the accountability of scientists to report violations of rules against using biology for destructive purposes; and (5) the promotion of these principles within oversight arrangements for dual-use research and publications. More than seventy member academies have endorsed the IAP approach.[97]

In the United Kingdom, the Royal Society has supported codes of conduct both as a means of raising consciousness among scientists about the potential for misuse of their work and as a focal point for training and education on relevant national and international obligations. The society also has argued for more-detailed codes of practice built on existing biosafety laws and regulations to help prevent the misuse of scientific research.[98] Codes of conduct also have been proposed by national science bodies in Germany and the Netherlands.

96. Brian Rappert, "Towards a Life Sciences Code: Countering the Threat from Biological Weapons," Strengthening the Biological Weapons Convention Briefing Paper no. 13 (2nd ser.), University of Bradford, Bradford, UK, September 2004, http://www.brad.ac.uk/acad/sbtwc/briefing/BP_13_2ndseries.pdf.

97. The InterAcademy Panel, "IAP Statement on Biosecurity," November 7, 2005, http://www.interacademies.net/10878/13912.aspx; and Jo L. Husbands, "Engaging the International Scientific Community in Issues of Dual-Use Research: The Experience of the NAS and the InterAcademy Panel" (presentation at The Advancement of Science and the Dilemma of Dual Use: Why We Can't Afford to Fail, Warsaw, November 9–10, 2007).

98. See, for example, Royal Society, *The Roles of Codes of Conduct in Preventing the Misuse of Scientific Research* (London: Royal Society, June 2005), https://royalsociety.org/~/media/Royal_Society_Content/policy/publications/2005/9645.pdf.

In the United States, the NSABB outlined the possible elements of a code of conduct in an appendix to its 2007 dual-use oversight framework, identifying the most important individual, group, and institutional responsibilities at each stage of the research process. The NSABB later developed an education module on dual-use research for scientists and a toolkit to help scientists formulate and disseminate a code of conduct.[99]

Professional associations such as the International Union of Microbiological Societies and the American Society of Microbiology (ASM) also have adopted codes of conduct. These codes have several common features: a commitment to biosafety, support for the ethical conduct of research, and opposition to the misuse of microbiology, including for development of biological weapons.[100] All of these codes, however, are general in nature.

The same is true of the only government code known to have been developed and promulgated for scientists and scientific institutions, the British code of ethics. This voluntary code, which was issued in 2007, contains a small number of broad principles: rigor, honesty, and integrity; respect for life, the law, and the public good; and, responsible communication, listening, and informing.[101]

Restrictions on the Dissemination of Information

Since September 11 and the anthrax letters, both scientists and scientific journals have been concerned about the possibility of restrictions on the dissemination of scientific findings that could have security implications. U.S. scientific journals have tried to forestall government-imposed restrictions, offering instead to establish their own review processes for handling sensitive manuscripts. The first to do so were the scientific journals published by the ASM, which in August 2002 began to require peer reviewers to inform journal editors of any manuscript that contained information on methods or materials that might be misused or pose a threat to public health or safety. The manuscripts would then be reviewed by the editor in chief in consultation with the ASM publications board. A few months later, the *Proceedings of the National Academy of Sciences* quietly adopted a similar process for reviewing manuscripts involving select agents. This was followed in January 2003 by a statement from thirty journal editors and scientists calling for the development of processes for considering the security implications of proposed manuscripts and, where necessary, for modifying

99. National Science Advisory Board on Biosecurity, *Enhancing Responsible Science—Considerations for the Development and Dissemination of Codes of Conduct for Dual Use Research* (Washington, D.C.: NSABB, February 2012), http://osp.od.nih.gov/sites/default/files/resources/COMBINED_Codes_PDFs.pdf.

100. Australian Society for Microbiology, "Ethics" (1979), http://www.theasm.org.au/about-us/governance/; American Society for Microbiology, "Code of Ethics" (2005), http://www.asm.org/index.php/governance/code-of-ethics; and International Union of Microbiological Societies, "Code of Ethics" (2008), http://www.iums.org/index.php/code-of-ethics.

101. United Kingdom, Government Office for Science, *Rigour, Respect and Responsibility: A Universal Ethical Code for Scientists* (London: Government Office for Science, September 2007), http://virtualbiosecuritycenter.org/wp-content/uploads/2012/07/UK-ethical-code.pdf.

or refraining from publishing papers whose potential harm outweighed their potential benefits. None of these initiatives, however, included guidance for reviewers on how to identify information that constituted a potential threat.[102]

In 2005 the limits of the journal editors' approach was put to the test when research involving the 1918 H1N1 virus was submitted to *Science* for publication. The NSABB was asked for its opinion and recommended publishing the paper after adding information on the public health benefits of the research. However, Donald Kennedy, *Science*'s editor in chief, later made clear that unless the paper had been classified he would have proceeded with publication, irrespective of the NSABB's recommendation.[103] Michael Osterholm, an NSABB member at the time, subsequently regretted the NSABB decision, arguing that if the reconstructed H1N1 virus had escaped the lab it could have caused a 1918-like pandemic, contrary to the NSABB's original assessment.[104]

In 2011, the NSABB again was asked for publication advice, this time on the work involving the construction of modified H5N1 viruses capable of respiratory transmission in mammals. But instead of supporting full publication, the NSABB recommended redacting methodological and other experimental details that could enable the modified viruses to be recreated and used to cause harm.[105] The NSABB also called for an international meeting of experts to discuss H5N1 research policy. Although WHO quickly organized the meeting, the participants were, as Osterholm later noted, from the "involved influenza research community, telling us what they should and shouldn't be allowed to do" based on their own self-interest.[106] The WHO experts group concluded that trying to limit access to the complete manuscripts would pose insurmountable practical problems, though it acknowledged the potential value of developing a mechanism for controlling access to other dual-use research information in the future.

After the WHO meeting, the U.S. government asked the NSABB to reconsider the two H5N1 manuscripts, which had been edited at the request of NIH to clarify the public health benefits of the research and the laboratory safety measures taken with the virus. Given what was in effect a choice between publishing the full manuscripts or none at all, the NSABB voted unanimously in one case and 12–6 in the other for publication. Paul Keim, another former

102. As discussed in Elisa Harris and John Steinbruner, "Scientific Openness and National Security after 9-11," *CBW Conventions Bulletin* (67) (March 2005): 1–6.

103. Donald Kennedy, "Better Never than Late," *Science* 310 (5746) (October 14, 2005): 195.

104. Michael T. Osterholm to Amy Patterson, April 12, 2012, https://labs.fhcrc.org/cbf/Papers/H5N1_docs/Osterholm_Letter_April_2012.pdf.

105. For a discussion of the handling of these manuscripts, see *Biological Security: The Risk of Dual-Use Research: Hearing before the Committee on Homeland Security and Governmental Affairs, United States Senate, One Hundred Twelfth Congress, Second Session*, 112th Cong. (2012) (statement of Anthony S. Fauci, Director, National Institute of Allergy and Infectious Diseases, National Institutes of Health), http://www.hsgac.senate.gov/download/2012-04-26-fauci-testimony-biological-security.

106. Osterholm to Patterson.

NSABB member, later commented that disinterested parties needed to be part of the process, as scientists could not be expected to assess the risks of their research on their own. Osterholm was more scathing, charging that the NSABB was continuing to "kick the can down the road" instead of figuring out how to manage DURC and its dissemination.[107]

Following the H5N1 controversy, NIH agreed to explore the feasibility of a mechanism for restricting access to sensitive dual-use information. This apparently was done as part of the review process that led to the U.S. government policies for oversight of DURC.[108] But rather than a mechanism for controlling access, NIH instead developed guidance for communicating DURC responsibly, including points for institutions and researchers to consider in assessing the risks and benefits of communicating their work. The guidance included an option for restricting access to sensitive information, but was silent on how institutions and researchers should do this.[109]

ASM journal editors also have acknowledged the difficulties of identifying and handling dual-use research information. In 2013–2014 the journals used the new U.S. government DURC policy to review several HPAI gain of function manuscripts. They concluded that determining whether an experiment meets the U.S. government definition of DURC is a judgment call and thus problematic for journal editors and IBCs. Presumably the same is true, but to an even greater extent, for researchers. In an unprecedented step, the editors, two of whom had served on the NSABB, called in April 2014 for the creation of a federal advisory board similar to the RAC to provide a more organized approach to managing DURC and its dissemination.[110]

GOVERNANCE CHALLENGES

Governments have traditionally viewed the risks posed by advances in the life sciences as a biosafety matter involving legitimate scientists or as a proliferation problem focused on national biological weapons programs. The former is reflected in the variety of international and national measures governing the handling and use of biological agents, such as the WHO biosafety manual, the

107. Brendan Maher, "The Biosecurity Oversight," *Nature* 485 (7399) (May 24, 2012): 431–434; and Osterholm to Patterson.

108. Kathryn Harris, Biosecurity and Biosafety Program, National Institutes of Health, personal correspondence, July 13, 2015.

109. National Institutes of Health, *Tools for the Identification, Assessment, Management, and Responsible Communication of Dual Use Research of Concern: A Companion Guide to the United States Government Policies for Oversight of Life Sciences Dual Use Research of Concern* (Washington, DC: National Institutes of Health, September 2014), 48–53, http://www.phe.gov/s3/dualuse/Documents/durc-companion-guide.pdf.

110. Arturo Casadevall, Terence S. Dermody, Michael J. Imperiale, Rozanne M. Sandri-Goldin, and Thomas Shenk, "On the Need for a National Board to Assess Dual Use Research of Concern," *Journal of Virology* 88 (12) (2014): 6535–6537.

NIH Guidelines, and the EU's biosafety regulations and directives. The latter is reflected in the conclusion of the BWC and in the subsequent multilateral and national efforts to deny proliferators access to biological materials, equipment, and related information through initiatives such as the Australia Group, export controls, and threat reduction programs in the former Soviet Union.

However, the September 11 terrorist attacks and the anthrax letters profoundly altered perceptions of the biological threat. To a greater degree than ever before, advances in the life sciences were viewed as not only a force for public good but also as a potential source of harm, particularly if used by terrorists or other nonstate actors. In response, further governance efforts concentrated first on what could be achieved most quickly: preventing unauthorized access to the most dangerous biological agents and toxins. In the United States, this meant stronger laws (the 2001 PATRIOT Act and 2002 bioterrorism bill) criminalizing biological weapons development and possession and regulating individuals and facilities that possess or use select biological agents or toxins. Over time, it also meant trying to keep pace with advances in technology (by screening gene sequence orders and including synthetic nucleic molecules in the *NIH Guidelines*) and with the diffusion of technology (by expanding threat reduction programs beyond the former Soviet Union). Internationally, it resulted in similar measures aimed at controlling access to specified biological agents and toxins (e.g., the 2001 UK antiterrorism law) and at strengthening the security of biological agents and toxins (e.g., UNSCR 1540, the OECD's biosecurity guidelines, and the INTERPOL bioterrorism prevention program).

On its own, each of the governance measures discussed in this chapter has a role to play in helping address one or more of the risks posed by dual-use biological materials, equipment, and related information. Together, they help create a web of prevention—against accidental harm to human beings or the environment from the research activities of legitimate scientists, as well as against deliberate harm to human beings, animals, or plants from the acquisition and use of biological agents or toxins by national governments, terrorists or other nonstate actors.

Few question the harm that could be caused by a dedicated national biological weapons program. A landmark 1993 U.S. Office of Technology Assessment proliferation study, for example, estimated that 1,000,000 to 3,000,000 deaths could result in a metropolitan area like Washington, D.C., if one hundred kilograms of anthrax spores were delivered as an aerosol from a single aircraft, under optimal dispersal and weather conditions, against an unprotected population.[111]

Of course deaths are not the only measure of harm. A proliferator's use of biological weapons could also have a severe economic impact, depending on the agent used, the delivery conditions, and the availability of post-attack prophylaxis. CDC scientists estimated in 1997 that the cost of an aerosol release

111. U.S. Congress, Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction: Assessing the Risks*, OTA-ISC-559 (Washington, D.C.: U.S. Government Printing Office, 1993), 52–54.

of anthrax spores in the suburbs of a major city could be up to $26.2 billion for every one hundred thousand people exposed. This estimate included only the casualty-related costs: lost future earnings, hospitalization, treatment, and so on. It did not include the decontamination or other costs associated with remediation after an attack or the broader costs to businesses and the economy from the disruption caused by the attack.[112]

No terrorist group or nonstate actor is known to have the technical and operational capabilities required to prepare and disseminate a large quantity of anthrax or other biological agent in an aerosol form. However, a more rudimentary terrorist capability, like that considered in a 2004 U.S. Homeland Security Council scenario, would still result in significant human and economic costs. Under this scenario, five cities were attacked sequentially by a truck disseminating an anthrax aerosol from a concealed, improvised spraying device. These attacks resulted in an estimated 328,848 exposures, 13,208 fatalities, and a further 13,342 casualties.[113]

Proliferators and terrorists are not the only potential sources of harm. Today, scientists have the capacity to resurrect extinct pathogens, as U.S. scientists did in the case of the 1918 HIN1 virus, which is estimated to have killed some 50 million people during the 1918 pandemic. Scientists can also modify existing pathogens to make them more dangerous, as Dutch scientists did when they made the highly lethal H5N1 avian influenza virus capable of respiratory transmission in mammals. And they can use synthetic biology to create novel pathogens, either by reengineering existing pathogens or by assembling nonliving biological components in novel ways. The accidental release of such pathogens could lead to devastating losses, human and financial.

This last source of potential harm is now overtaking biological weapons proliferation and bioterrorism as a primary concern. The latest U.S. government report on arms control treaty compliance, released in June 2015, raises questions about biological research and development activities in Russia and Iran and about whether North Korea and Syria still consider the use of biological weapons as a military option. But no country is charged with maintaining a biological weapons program.[114] Similarly, eight years after the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism predicted that a terrorist incident with biological weapons would likely occur by the end of 2013, concerns about bioterrorism gradually are being replaced

112. A. F. Kaufmann, M. I. Meltzer, and G. P. Schmid, "The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable?" *Emerging Infectious Diseases* 3 (2) (April–June 1997): 83–94, http://wwwnc.cdc.gov/eid/article/3/2/97-0201.

113. Homeland Security Council, "Scenario 2: Biological Attack—Aerosol Anthrax," in *Planning Scenarios: Executive Summaries*, 2–1–2 (Washington, D.C.: Homeland Security Council, July 2004), http://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04.htm#toc.

114. Department of State, "2015 Report on Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments," June 5, 2015, http://www.state.gov/t/avc/rls/rpt/2015/243224.htm#BWC2.

by broader concepts of biorisk and health security, which bring together all biological threats, whether deliberate, accidental, or natural in origin.[115]

What may now be the most serious source of potential harm is also subject to the weakest governance efforts. Despite more than a decade of meetings, discussions, and reports, little progress has been made toward achieving effective national measures or common international policies for overseeing the most consequential areas of dual-use life sciences research. Proposals have been made by the Fink Committee, the NSABB, and others in the United States, as well as by science and ethics bodies in the United Kingdom, the Netherlands, and Germany to include all relevant research in the oversight process and to work to harmonize these policies internationally. But thus far, serious challenges have prevented these proposals from being adopted.

The first and perhaps most important challenge is from scientists themselves. Surveys from 2004 to 2007 found that U.S. scientists believe the select agent requirements pose a burden, affecting their ability to collaborate domestically and internationally and increasing the time and financial costs of conducting research.[116] Fears that scientists would abandon much-needed life sciences research, including work with select agents, led many scientists to endorse self-governance of life sciences research as an antidote to government regulation. In the United States, this bias toward self-governance was a dominant feature of the NSABB's initial recommendations for oversight of dual-use research. As Paul Keim later observed in response to criticism over the NSABB's handling of the H5N1 manuscripts, "We're accused of being the bad guys. But most of what we've done is to push back against harsher regulations."[117] Self-governance has also been at the heart of the limited policies that the U.S. government finally began to put in place in 2012, more than five years after the NSABB released its DURC oversight recommendations. Internationally, the challenge from scientists can be seen in the priority given by WHO and other science bodies to raising awareness among life scientists through training and education in biosafety and biosecurity as well as through voluntary codes of conduct. Scientists, the argument went, were in the best position to assess the risk of their own work, and creating a culture of responsibility would facilitate this process.

115. In addition to predicting a biological weapons terrorist attack, the commission also emphasized that, given the technical expertise required to carry out a large-scale biological attack, the United States should "be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists." Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, *World at Risk* (New York: Vintage Books, 2008), xv, 11; and Al Mauroni, "Gauging the Risk from Bioterrorism," *War on the Rocks*, June 2014, http://warontherocks.com/2014/01/gauging-the-risk-from-bioterrorism/.

116. As discussed in M. Beatrice Dias, Leonardo Reyes-Gonzalez, Francisco M. Velosoa, and Elizabeth A. Casman, "Effects of the USA PATRIOT Act and the 2002 Bioterrorism Preparedness Act on Select Agent Research in the United States," *Proceedings of the National Academy of Sciences* 107 (21): 9556–9561.

117. Heidi Ledford, "Call to Censor Flu Studies Draws Fire," *Nature* 481 (7379) (January 5, 2012): 9–10.

Many of the predicted negative effects on select agent research in the United States that helped encourage the push for self-governance of dual-use research do not seem to have been borne out. In a study published in 2010, investigators reported an overall stimulus to the field after 2002, based on an archival review of the number of *Bacillus anthracis* and Ebola virus "papers published per year, number of researchers authoring papers, and influx rate of new authors." Even after controlling for the increased funding available for select agent research after 2001, the study found an increased propensity for U.S. authors to begin select agent research. Domestic collaborations on select agent research also increased, as did international partnerships with certain foreign research institutions. The most significant negative effect was a loss of efficiency: the number of research papers published per million dollars of select agent funding declined two- to five-fold.[118]

In the United States, effective governance of biotechnology research has also been challenged by the sharp increase in biodefense spending since September 11. Much of this funding has been for research on medical countermeasures to protect against deliberate biological attacks. At the NIH, for example, funding for civilian biodefense, which excludes military biodefense spending, increased from a modest $53 million in fiscal year (FY) 2001 to $6.72 billion (budgeted) for FY 2016.[119] In the first few years of this expansion, from 2001 to January 2005, the number of NIH-funded research grants on anthrax, plague, and other potential biological warfare agents jumped to almost five hundred from thirty-three between 1996 and 2000.[120] NIH also created a broad network of facilities to support its biodefense work, including eleven Regional Centers of Excellence (RCEs) for biodefense and emerging infectious diseases research; two national and twelve regional biocontainment laboratories for research requiring high levels of containment; and, most recently, fourteen Centers of Excellence for Translational Research (CETR) on medical countermeasures or related technology, which have replaced the RCEs. These laboratories were part of a broader expansion of U.S. high-containment laboratories from slightly

118. Beatrice Dias et al., "Effects of the USA PATRIOT Act."

119. Tara Kirk Sell and Matthew Watson, "Federal Agency Biodefense Funding, FY2013–FY2014," *Biosecurity and Bioterrorism* 11 (3) (September 2013): 196–216; and Crystal Boddie, Tara Kirk Sell, and Matthew Watson, "Federal Funding for Health Security in FY2016," *Health Security* 13 (3) (2015): 186–206. The figure of $6.72 billion for FY 2016 includes $1.37 billion for civilian biodefense and $5.35 billion for multiple hazard and preparedness line items previously included as civilian biodefense funding by Boddie, Sell, and Watson.

120. *Biodefense: Next Steps: Hearing before the Subcommittee on Bioterrorism and Public Health Preparedness of the Committee on Health, Education, Labor, and Pensions, United States Senate, One Hundred Ninth Congress, First Session*, 109th Cong. (2005) (prepared statement of Anthony S. Fauci, Director, National Institute of Allergy and Infections Diseases, National Institutes of Health), https://www.gpo.gov/fdsys/pkg/CHRG-109shrg98930/pdf/CHRG-109shrg98930.pdf.

more than four hundred in 2004 to an estimated fifteen hundred today.[121] Across the U.S. government, funding for civilian biodefense exceeded $90 billion from FY 2001 to FY 2016.[122]

Although the Fink Committee singled out biodefense research as raising particular dual-use concerns, neither the oversight approach it recommended nor that proposed by the NSABB clearly apply to military biodefense work, given the decision by both to link dual-use oversight only to academic or other institutions formally subject to the *NIH Guidelines*. One of the RCEs established by NIH to conduct biodefense research, the Southeast RCE (SERCEB), initiated its own dual-use review process in 2004 for proposals it intended to fund. SERCEB identified two important issues in the course of its dual-use reviews: (1) that few investigators were aware of the dual-use problem; and (2) that technical expertise was critical to dual-use risk assessment. For these reasons, SERCEB cautioned against making researchers solely responsible for identifying whether their own research posed dual-use risks, noting that dual-use awareness is highly subjective.[123]

Classified biodefense work was explicitly exempted not only from the scope of the NSABB's work but, ultimately, from the dual-use oversight policies promulgated by the U.S. government in 2012 and 2014. According to the DOD, classified projects are not reviewed for dual-use concerns because the information and products from those projects are controlled through the classification process.[124] This reflects a profound misunderstanding of the purpose of dual-use review, which is to identify and mitigate risks not only from research results but from the research process itself. Whether DHS includes classified research projects in its dual-use review process is not known.

Finally, differing national perceptions of the risk from biotechnology research and of the importance of the issue in national policy have been a challenge to effective national and international governance efforts. For developing countries, the possible misuse of dual-use biological materials, equipment, or information is an abstract problem compared to the millions of people who die each year from naturally occurring diseases such as tuberculosis, malaria, and hepatitis. For these countries, the global diffusion of dual-use technology

121. As the Government Accountability Office has repeatedly pointed out, the exact dimensions of this laboratory expansion are not known, as only facilities that possess or transfer select agents must register with a government agency. Government Accountability Office, *High Containment Laboratories: Assessment of the Nation's Need Is Missing*, GAO-13-466R (Washington, D.C.: GAO, February 25, 2013), http://www.gao.gov/assets/660/652308.pdf.

122. Sell and Watson, "Federal Agency Biodefense Funding, FY2013–FY2014"; and Boddie, Sell, and Watson, "Federal Funding for Health Security in FY 2016." The $90 billion figure includes $78.82 billion reported in Sell et al. for FY 2001 through FY 2014; $3.05 billion reported in Boddie Sell, and Watson for FY 2015 and FY 2016; and $10.11 billion reported in Boddie, Sell, and Watson for FY 2015 and FY 2016 "multiple hazard and preparedness" line items previously included as civilian biodefense funding by the authors.

123. E. Megan Davidson, Richard Frothingham, and Robert Cook-Deegan, "Practical Experiences in Dual-Use Review," *Science* 316 (5830) (June 8, 2007): 1432–1433.

124. Walter B. Chase III, CTR OSD OUSD ATL, personal communication, June 19, 2015.

is critical not only to their ability to fight indigenous disease threats but to their economic and technological development more broadly. Concerns about the potential impact of biotechnology research are seen as a preoccupation of Western countries and, in some cases, as a veiled excuse for technology denial.

While developing countries generally do not share the West's dual-use concerns, even developed countries have been slow to embrace effective governance of all aspects of the dual-use problem. Long-standing biosafety measures coupled with efforts aimed at preventing national biological weapons programs were supplemented after September 11, 2001, with other initiatives designed to deny terrorists access to dangerous pathogens and toxins or equipment that could enable their production. National oversight of biotechnology and other research being conducted as part of the evolving revolution in the life sciences has been much more limited, emerging in only a few countries. Efforts to develop common international policies and procedures for overseeing the most consequential areas of dual-use research have been even less successful. This has been the case despite the fact that virtually every report by a scientific body on the dual-use biotechnology research issue over the past decade has underscored the international dimension of the problem and the corresponding need for an international response. From the Fink Committee to the British Royal Society to the WHO, the importance of harmonized international standards for managing dual-use research of concern has been repeatedly highlighted.

***

Many important steps have been taken over the past half-century to try to respond to the complex and multifaceted risks posed by dual-use biological materials, equipment, and related information. Although direct links cannot be drawn between specific measures and outcomes, most observers are likely to agree that, taken together, these measures have contributed to progress in preventing the acquisition of biological weapons, controlling access to biological weapons–related capabilities, and promoting the safe handling of dangerous biological materials. Most of these measures emerged in response to specific controversies or concerns. Opposition to the use of herbicides and riot control agents in Vietnam contributed to the conclusion of the BWC. Fears of recombinant DNA technology led to the *NIH Guidelines* and to EU directives controlling GMOs. Western assistance to Iraq's chemical and biological weapons programs resulted in the creation of the AG and the adoption of national controls on biological weapons–related capabilities. And post–Cold War worries about the proliferation of material and expertise from the former Soviet weapons program stimulated the CTR.

The September 11 terrorist attacks and subsequent anthrax letters were directly responsible for a wide array of other national and international measures. These include the U.S. select agent regulations and biological weapons criminalization provisions, the UK antiterrorism act, Danish and Israeli laws controlling dangerous pathogens and high-consequence research, and the Canadian law regulating human pathogens. Internationally, these measures

include UNSCR 1540, the G8 Global Partnership, the Proliferation Security Initiative, the INTERPOL bioterrorism prevention program, and the WHO and OECD biosecurity guidelines.

Even the limited measures that have been adopted in the United States to manage the risks from dual-use research emerged only after other controversies. The NSABB provided its recommendations on dual-use oversight in June 2007 but not until March 2012 did the U.S. government publish its first policy on the issue—and only then after controversy had erupted over the U.S. and Dutch H5N1 projects, which had been funded by NIH without considering dual-use concerns. The U.S. government's September 2014 institutional DURC policy was released in the midst of an unprecedented debate within the scientific community over GOF research and after a summer of revelations regarding U.S. laboratory incidents involving dangerous pathogens.

Given the wide range of challenges to effective oversight, it is difficult to imagine that policy-makers in the United States or other countries will support a robust approach to oversight of DURC in the absence of an event that makes effective oversight a more salient political issue. But perhaps that is too pessimistic. It is possible that the "deliberative process" now underway in the United States to develop a policy on the conduct and funding of GOF research will result in stronger oversight measures, at least for this particular type of research. In the near term, the most direct and expeditious way of achieving this is by adding GOF studies of concern to the restricted experiments section of the select agent regulations, which not only outline clear oversight requirements but are legally based. The possibility that other types of experiments might require more stringent scrutiny and need to be added to the restricted experiments was in fact explicitly acknowledged by both HHS and USDA in their regulations.[125]

Ultimately, however, more robust oversight arrangements need to be adopted for other types of DURC as well. To encourage compliance and adequate funding for implementation, the oversight requirement should be mandatory. To make it more effective, it should apply to all relevant research, whether academic, industry, or government, including classified biodefense or other projects. And to help researchers determine whether their proposed work is subject to oversight, the affected categories of research should be clearly defined. The Danish approach to dual-use research is one example of how this could be done: outlining the basic obligation, including the scope of application, in legislation but using executive actions (such as executive orders and policy guidance), which provide more flexibility for responding to technological developments, to enumerate the implementation details.

The oversight arrangements also should be coordinated by an independent federal entity, as the biosecurity working group established by President George W. Bush recommended in 2009. To build confidence, it should consult with but not be based within any of the government agencies that are responsible

125. This idea comes from Richard Ebright. See https://fas.org/blogs/secrecy/2015/10/restricted-experiments/.

for funding or conducting dual-use research. It should oversee and assess the progress and impact of the oversight requirements and, as the GOF ethical study suggested, provide an additional level of review of proposed research projects that raise the most serious concerns.

Finally, consistent with the globally distributed nature of life sciences research, the U.S. government should seek to establish common DURC rules and procedures internationally. This means going beyond mere discussions of biosecurity and biosafety in various international fora, as has been done for many years, and developing a concrete strategy for pursuing international harmonization of laws, regulations, and policies for the most consequential types of life sciences research. As the Fink Committee pointed out, this is essential if the risks from dual-use research are to be managed effectively. It also is essential to avoid U.S. scientists being put at a competitive disadvantage in relation to life sciences researchers in other countries.

Chapter 3

Governance of Information Technology and Cyber Weapons

Herbert Lin

FRAMING THE PROBLEM

In the twenty-first century, information is the key coin of the realm. Nations rely on information and information technology (IT) to ever-increasing degrees. Computers and networks are integral for most business processes, including payroll and accounting, tracking of sales and inventory, and research and development (R&D). Delivery of food, water, energy, transportation, healthcare, and financial services all depend on IT, which is itself a major sector of the economy. Modern military forces use weapons that are computer controlled. Coordination of actions of military forces depends on networks that allow information about the battlefield to be shared. Logistics for both civilian and military activities depend on IT-based scheduling and optimization.

But bad guys also use IT. Criminals use IT to steal intellectual property and commit fraud. Terrorists use IT for recruitment, training, communications, and public outreach, often in highly sophisticated ways, although to date they are not known to have used IT to commit destructive acts. And as the U.S. government is exploring various ways of using cyberspace as an instrument of national policy to create political, military, diplomatic, economic, or business advantages, other nations—some of them with interests that do not align with those of the United States—are doing the same.

One commonly used definition of *dual-use technology* is "technology intended for beneficial purposes that can also be misused for harmful purpos-

es."[1] This article focuses on the governance of *specific applications* of IT (or research aimed at developing such applications) designed and intended to create specific negative effects on a target's computer or communications system or the information inside it, being carried through it, or being processed within it and which can be used for both beneficial and harmful purposes. In the lexicon of this article, these specific applications are "cyber weapons."[2] The negative effects of possible concern are effects on integrity (in which data or computer operations are altered with respect to what users expect), effects on availability (in which services provided to users of the system or network are unavailable when expected), and effects on confidentiality (in which information that users expect to keep secret is exposed to others).

Note the distinction between *effects* and *purpose*. A gun is designed to have negative effects on objects and people. But in the hands of the good guys, (e.g., the police), its use is beneficial to society.[3] Guns are misused for harmful purposes primarily when they are put into the hands of the bad guys (e.g., criminals). Similar comments apply to applications of IT with negative effects. For example, a negative effect of a specific program might be to render ineffective the encryption capabilities of a targeted system. In the hands of the good guys, the purpose may be benign or societally beneficial—consider, for example, the properly authorized use of such a program by a law enforcement agency against a computer used by criminals. But if the same computer program performing the same task were used by a terrorist or criminal (e.g., used against a government computer containing classified information or a corporate computer holding confidential business plans), that purpose would be regarded as a harmful or nonbenign misuse.

When the use of a cyber weapon affects the integrity or the availability of a service, it is usually classified as a cyberattack. More generally, cyberattack refers to the use of cyber weapons to alter, usurp, deny, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or competitor or the information and/or programs resident in or transiting these systems or networks. The activities may also affect artifacts connected to these systems and networks—examples of such artifacts, often called cyber-physical devices, include

1. See, for example, National Research Council, *Biotechnology Research in an Age of Terrorism* (Washington, D.C.: National Academies Press, 2004); and Seumas Miller and Michael J. Selgelid, "Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences," *Science and Engineering Ethics* 13 (4) (2007): 523–580. The definition used in the life sciences contrasts with what might be called a "traditional" definition of dual-use technology; namely, technology that has both civilian and military applications. This traditional definition is used by the U.S. government (15 CFR 730.3) and the European Commission (see "Dual-Use Export Controls," updated January 28, 2016, http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/).

2. The term *weapon* is not entirely satisfactory in this context, since in noncyber contexts a weapon is usually an artifact that is used to destroy or damage human beings or other objects. However, this author knows of no other word that is any better, and many that are worse.

3. Although not all uses of guns by police are societally beneficial, such uses are not the intent of supplying guns to police officers.

generators, radar systems, and physical control devices for airplanes, automobiles, and chemical manufacturing plants. A cyberattack might be conducted to prevent authorized users from accessing a computer or information service (a denial of service attack), to destroy computer-controlled machinery, or to destroy or alter critical data (e.g., timetables for the deployment of military logistics).

When the use of a cyber weapon compromises the confidentiality of information that is intended to be kept secret from unauthorized parties, it is usually classified as a "cyber exploitation." (Press accounts often use the term *cyberattack* when the activity conducted is actually cyber exploitation.) More generally, *cyber exploitation* refers to the use of cyber weapons to obtain information resident on or transiting through a system or network. The information sought is information that the target wishes not to be disclosed. For a company, such information may include trade secrets, negotiating positions, R&D information, or other business-sensitive information. For a nation, such information may include intelligence information, the strength and disposition of military forces, military plans, communications with allied nations, and so on. Of particular interest is information that will allow the perpetrator to conduct further penetrations on other systems and networks to gather additional information.

In general, a cyber weapon requires both penetration and payload. (Selecting the targets on which cyber weapons are used is a matter of command and control of those weapons.)

Penetration requires a mechanism for gaining access to the system or network of interest (e.g., through the Internet, by physical intrusion) and taking advantage of a vulnerability in the system or network. Vulnerabilities may be accidentally introduced through a design or implementation flaw (often called a "bug"), or introduced intentionally (e.g., by an untrustworthy insider). Before a vulnerability is known to the supplier of the system or network (and thus before it can be repaired), a system with that vulnerability can be penetrated by an adversary who does know of it. When an adversary uses a vulnerability that is unknown to others to effect penetration, it is termed a "zero-day" penetration or compromise, since the victim will have had zero days to respond to it.

Payload is the term used to describe the mechanism for affecting the victim's system or network after penetration has occurred. The payload is a program that executes after the cyber weapon has entered the computer system of putative interest;[4] payload execution may result in the weapon reproducing and retransmitting itself, destroying files on the system, or altering files. Payloads can be designed to do more than one thing, and these things can happen at different times. If a communications channel is available, payloads can be remotely updated. (And in some cases, the function of the payload is performed by a human being who has gained remote access to the computer in question through use of a penetration mechanism.)

4. The qualifier "of putative interest" accounts for the possibility that the payload may find itself in a computer system that the attacker did not intend to attack; in this case, payload execution may have negative effects on the wrong system.

From the standpoint of the victim, one of the most problematic aspects of cyber weapons arises from the fact that the payload—and only the payload—determines whether the weapon is used for damaging or destructive actions (attacks) or nondestructive actions (exploitation/espionage). Even after recognizing an intrusion into a system or network, the victim usually cannot be certain whether the purpose of that intrusion is destructive or nondestructive.[5]

Some of the most important characteristics of cyber weapons are as follows:

- The use of a cyber weapon can lead to results that vary from the utterly insignificant to destruction over a large scale. Similarly, the duration and spatial scale of a cyber weapon's impact can span many orders of magnitude. But any given cyber weapon almost certainly is not designed to span such a range.
- A given cyber weapon can often be used only once because a penetration that takes advantage of a system or network vulnerability usually reveals the vulnerability. If the victim repairs the vulnerability, a later use of the same weapon may not succeed.
- Obtaining a large-scale and long-lasting impact from the use of a single cyber weapon can be highly challenging. Large-scale impact may well require simultaneous attacks against a large number of heterogeneous targets, and such heterogeneity means that a different attack would have to be crafted against each target type. Long-lasting impact may require repeated strikes against the targets of interest, and any vulnerability whose presence resulted in serious negative effects is likely to be repaired quickly, making that vulnerability unusable in the future.
- The effects of using a cyber weapon may or may not be significantly delayed in time from the moment of penetration. That is, the payload may not execute immediately once penetration has been effected.
- The successful use (launch) of a cyber weapon generally depends heavily on accurate, detailed, and timely information about the target (and what is connected to it). Such information may be gathered through the use of a variety of methods, including the use of other cyber weapons. In the absence of such information, the use of any given cyber weapon may have no effect whatsoever.
- The effects of using a cyber weapon remain unknown until the payload executes (or until all of the payload is available for analysis).
- The use of a cyber weapon is plausibly deniable under many circumstances—the so-called attribution problem. High-confidence attribution

5. In some contexts, certain forms of espionage—for example, involving ships, submarines, or aircraft as the collection platforms—have been seen as military threats, so the mere fact that a given action might count as espionage (among other things) does not mean that the action in question must be regarded as "only" espionage. See, for example, Roger D. Scott, "Territorially Intrusive Intelligence Collection and International Law," *Air Force Law Review* 46 (1999): 217–226, http://www.afjag.af.mil/shared/media/document/AFD-090108-036.pdf.

of such use to an entity that can be held responsible is most difficult when the weapon in question has never been used before (which means there is no historical record with which to compare), when the responsible entity has maintained perfect operational security (which means the victim has no other sources of intelligence on which to make a judgment), and when the judgment needs to be made quickly. Conversely, when these conditions are not true, attribution is often much easier.

- A given cyber weapon may or may not be self-propagating. Self-propagation refers to the ability of software to duplicate itself on one system and then to take advantage of connections to other systems to spread to those systems. Depending on the weapon's programming, self-propagation may be limited or unlimited. To the extent that the computing environments of affected systems constitute a monoculture, self-propagation is dangerous because the same program can affect all of the systems involved. But if the relevant computing environments are different from one another, similar effects on all of the systems are unlikely to be the result. A cyber weapon that is not self-propagating affects only the system against which it is targeted, except to the extent that failures in that system may affect other systems connected to it.
- The expertise and infrastructure needed to create certain kinds of cyber weapons extend beyond the usual purview of computer scientists. Cyber weapons that are intended to be used against cyber-physical systems—systems or devices that are controlled by computer but have tangible effects in the physical world—also require expertise specific to those systems or devices and also, under some circumstances, test facilities that are a high-fidelity replica of the targets to be attacked. (For example, the Stuxnet worm used to attack Iranian centrifuge facilities was previously tested on facilities located at Dimona, the Israeli nuclear complex in the Negev Desert.[6])

Because cyber weapons can be used for beneficial purposes (i.e., by the good guys) and misused for harmful purposes (i.e., by the bad guys), cyber weapons constitute a dual-use technology of concern. But unlike the case for the analogous dual-use technology in biology (for which there is a well-established consensus that the use of a biological weapon would *define* the user as a bad guy), what makes the use of a cyber weapon harmful is very much in the eyes of the beholder.

For example, consider technologies that make it easier for nations to spy on one another. Most nations conduct espionage operations on other nations, and yet no nation wants other nations to conduct similar operations against it. From Nation A's perspective regarding Nation B, A's use of espionage against

6. William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

B serves a beneficial purpose, whereas B's use of espionage against A serves a harmful purpose. Of course, Nation B believes the opposite.

The nations of the world have not agreed that the use of cyber weapons is ipso facto a harmful use, nor have they agreed that only bad guys use cyber weapons or that the development and acquisition of cyber weapons is necessarily something to be avoided.[7] For these reasons, much of the governance discussion in this chapter explores what the world does and does not believe about cyber weapons.

A second example comes from the email people routinely receive. A substantial portion of email traffic consists of "spam"—unsolicited commercial email that is sent in bulk. For the vast majority of recipients, such emails are annoying and in effect constitute a denial of service attack on them. Recipients waste time deleting these emails in search of useful emails in their traffic. But for the senders of such email and a small proportion of those who receive it, the email is beneficial. Senders earn some profit from sending the emails, and some individuals want the products or services offered and respond affirmatively.

So what are the beneficial purposes of cyber weapons? Perhaps the most important purpose is to assist defenders in testing themselves against adversaries. That is, if I want to strengthen my system against a cyber onslaught, I need to take specific measures—and then I need to test my upgraded system to see if indeed it is more robust. Knowledge of possible offensive techniques (using cyber weapons) helps me to design a better defense—and my refraining from developing specific cyber weapons is no assurance that others will do the same.

Who uses cyber weapons for harmful purposes? The range of possible users is large and includes lone hackers acting as individuals; criminals acting on their own for profit; organized crime (e.g., drug cartels); transnational terrorists (perhaps acting with state sponsorship or tolerance); small nation-states; and major nation-states. Moreover, today one can find service providers who will, for a fee, use cyber weapons against targets of the customer's choosing. The availability of such services enables any party with the appropriate financial resources to cause negative cyber effects, even if that party has no particular technical expertise.

Motivations for using cyber weapons in such operations also span a wide range. One of the most common motivations is financial. Cyber exploitations can yield valuable information, such as credit card numbers or bank log-in credentials; trade secrets; business development plans; or contract negotiation strategies—such information can be sold. Cyberattacks can disrupt the production schedules of competitors, destroy valuable data belonging to a competitor, or be used as a tool to extort money from a victim.

Another possible motivation is political. A perpetrator might use cyber weapons to advance some political purpose. A cyberattack or exploitation may

7. At times during the Cold War, both the United States and the Soviet Union advocated peaceful applications of nuclear explosives. Although the idea of such applications has largely fallen out of favor, some nations apparently continue to advance that position. Still, the taboo against nuclear explosions—for whatever purpose—is much stronger and globally widespread than any existing norms of behavior regarding the use of cyber weapons.

be conducted to send a political message to a nation, to gather intelligence for national purposes, to persuade or influence another party to behave in a certain manner, or to dissuade another party from taking certain actions.

Still another reason for conducting such operations is personal. The perpetrator might conduct the operation to obtain "bragging rights," to demonstrate mastery of certain technical skills, or to satisfy personal curiosities.

Lastly, the use of cyber weapons could be integrated into military operations in much the same way as kinetic weapons. In such scenarios, cyber weapons become just another weapon that military commanders might use—in this case, to damage either the system or network directly targeted or the devices connected to it. Individuals with no military affiliation may also wish to use cyber weapons for physically destructive purposes for reasons such as maliciousness, extortion, or financial gain.

A focus on the governance of cyber weapons means that other governance measures that promote cyber defenses—applications of IT intended to thwart or respond to the operation of cyber weapons—are not central to this chapter. In the big picture of efforts to promote and enhance cybersecurity, this is a big omission, as the vast majority of work on cybersecurity and related governance measures is defensively oriented. But since the vast majority of defensive applications are regarded as benign and because few parties feel a need to govern benign activities, they fall outside this chapter's ambit.[8] Therefore, this chapter does not address governance measures focused on defense, such as measures to improve coordination of defensive responses to cyberattacks, to promote and enhance cooperative relationships among law enforcement authorities in different nations in order to enhance their ability to respond to cyberattacks, or to build stronger and more resilient cyber infrastructures. Such measures—and others—are unquestionably important to the governance of security in cyberspace, but the issues associated with the governance of security in cyberspace constitute a vastly larger set than those associated with cyber weapons per se.

Moreover, the technical specifics of cyber defenses are not in general closely related to the specific details of cyber weapons. For example, a cyber defense may look for the known "fingerprint" of a penetration mechanism, but the part of the weapon that does the actual harm is its payload (which may not even be present at the time the penetration mechanism is recognized). In this regard, cyber defenses share a characteristic with nuclear defenses, which are more properly characterized as defenses against the delivery systems that could carry nuclear weapons rather than against the nuclear weapons themselves. But with one notable exception, cyber defenses do not seek to mitigate damage caused by the use of cyber weapons. (The exception is that encryption mitigates harm caused by cyber exploitation. Adversaries may obtain encrypted information,

8. The allegedly benign nature of defensive applications of IT warrants one important point of clarification. A defensive application will just as easily protect a computer operated by a hostile nation as one operated by or in a friendly nation, and it serves friendly interests if the former computer remains vulnerable. Export controls of various kinds seek to impede the transfer of certain defensive applications to hostile nations.

but that information is useless to them without a way to decrypt it.) Cyber defenses are thus dissimilar to biological defenses such as antimicrobial drugs or vaccines, which are developed to mitigate damage caused by biological agents (of either natural or deliberate origin).

Techniques and approaches that protect against deliberately induced failures in IT (i.e., that protect against cyber weapons) are also often useful against failures in IT that are not deliberately induced. For example, the Morris worm of 1988 was a self-replicating, self-propagating program that was released onto the Internet. The author, Robert Morris, had intended the program to spread onto systems that were previously untouched by the program, but only once. An error in the program caused it to replicate numerous times on the systems it touched, thereby crashing those systems. The program eventually spread to a large number of systems on the Internet (around 6,000, or about 10 percent of the Internet-connected systems at the time). The program took advantage of vulnerabilities in existing programs on those systems. Had those vulnerabilities been repaired or never been introduced, the program would not have been successful at spreading to even one machine.

An additional question remains: Given its potential for beneficial and harmful uses, should IT itself be regarded as a dual-use technology? The answer is no, at least in the sense that one would not logically regard physics or biology in the same way. Physics, biology, and IT can be used to create a broad range of applications, only some of which raise dual-use concerns. Pencils and walkie-talkies are applications of IT, and in the hands of criminals or terrorists they are often used to facilitate the commission of crimes and other terrorist acts. Yet the public has expressed little concern about the misuse of pencils and walkie-talkies for harmful purposes.

More generally, IT is often regarded as a medium for expressing thoughts. As described in a 1992 NRC report on the future of computer science, "Computer programs enable the computer scientist and engineer to feel the excitement of seeing something spring to life from the 'mind's eye' and of creating information artifacts that have considerable practical utility for people in all walks of life."[9]

Fred Brooks, arguably one of the fathers of modern computing, writes, "The programmer, like the poet, works only slightly removed from pure thought-stuff. He builds castles in the air, creating by the exertion of the imagination. . . . Yet the program construct, unlike the poet's words, is real in the sense that it moves and works, producing visible outputs separate from the construct itself. . . . The magic of myth and legend has come true in our time.

9. National Research Council, *Computing the Future: A Broader Agenda for Computer Science and Engineering* (Washington, D.C.: National Academies Press, 1992), http://www.nap.edu/catalog/1982/computing-the-future-a-broader-agenda-for-computer-science-and. See also *Computer Science: Reflections on the Field, Reflections from the Field* (Washington, D.C.: National Academies Press, 2004); and William J. Mitchell, Alan S. Inouye, and Marjory S. Blumenthal, eds., *Beyond Productivity: Information, Technology, Innovation, and Creativity* (Washington, D.C.: National Academies Press, 2003).

One types the correct incantation on a keyboard, and a display screen comes to life, showing things that never were nor could be."[10]

If IT is indeed a general-purpose medium for expression, meaningful "governance" of such a technology is hard to imagine. That said, a question still remains regarding the existence of specific areas of research in IT where progress may help to enable the creation or improvement of cyber weapons.

PAST USES OF CYBER WEAPONS

Past uses of cyber weapons have encompassed a wide range of criminal activities (for example, use of cyber weapons to steal money, commit fraud, or appropriate trade secrets that constitute intellectual property), activities that are aimed at obtaining national security information (for example, use of cyber weapons by one nation to conduct espionage against another), and activities that are destructive in nature (for example, use of cyber weapons to destroy data, render information systems inoperable, or damage machinery controlled by computers).

Some of the more notable instances in which cyber weapons have been used include the following.[11]

- A denial of service attack in 2007 against Estonian government websites, media sites, and online banking services prevented citizen access to these sites and services for an extended period of time. The attack is widely believed to have originated in Russia, though whether the attack was launched at the explicit behest of the Russian government is less clear.
- Stuxnet, a cyberattack conducted in 2009 and 2010, destroyed about one thousand Iranian uranium enrichment centrifuges.[12] The United States and possibly Israel are widely believed to have been responsible for the attack.
- In August 2012, Aramco, the national oil firm of Saudi Arabia, was struck by a cyberattack that wiped out the data and operating systems on thirty thousand computers connected to the Aramco network.[13] Accord-

10. Frederick Brooks, *The Mythical Man-Month* (Reading, Mass.: Addison-Wesley, 1975).

11. A more complete list of notable international cyber events can be found in Catherine A. Theohary and Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, CRS Report R43848 (Washington, D.C.: Congressional Research Service, January 5, 2015), https://www.hsdl.org/?view&did=761572.

12. For a primer on Stuxnet, see "Cyberattacks on Iran—Stuxnet and Flame," *New York Times*, n.d., http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?scp=1-spot&sq=stuxnet&st=cse.

13. Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

ing to press reports, the United States believes Iran was responsible for the attack.

- A denial of service attack in the fall of 2012 against U.S. banks caused significant delays for users trying to access online banking sites.[14] Some analysts believe that the government of Iran tolerated or encouraged these attacks, though the extent of its responsibility is unclear.
- In June 2013 the U.S. Department of Defense acknowledged that sensitive unclassified data regarding the F-35 fighter jet had been stolen, significantly reducing the U.S. design and production edge on fifth-generation fighters (e.g., cost advantage and lead time) compared to other nations that are seeking to produce such fighters.[15]
- In December 2013, Target reported a data breach involving the credit and debit card records of more than 40 million customers, as well as personal information such as email and mailing addresses for some 70 million people. The access path used by the intruders involved one of Target's HVAC service vendors. The vendor apparently had access to the entire Target network.[16]
- In May 2014 the U.S. Justice Department issued indictments against five members of the Chinese People's Liberation Army for violations of the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act, alleging that these individuals engaged in criminal acts of industrial espionage that took place in the 2006–2014 period.[17]
- In September 2014, Home Depot reported that about 56 million credit and debit cards had probably been compromised over a six-month period earlier that year through malicious software implanted on point-of-sale terminals.[18]
- In November 2014, Sony Pictures Entertainment was the victim of a cyberattack that compromised unreleased films, private email correspondence, and other sensitive information and also destroyed operating sys-

14. Nicole Perlroth, "American Banks Undamaged by Cyberattacks," *Bits* (blog), *New York Times*, September 26, 2012, http://bits.blogs.nytimes.com/2012/09/26/american-banks-undamaged-by-cyberattacks/.

15. David Alexander, "Theft of F-35 Design Data Is Helping U.S. Adversaries—Pentagon," Reuters, June 19, 2013, http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619.

16. Nicole Perlroth, "Heat System Called Door to Target for Hackers," *New York Times*, February 5, 2014, http://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html.

17. Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

18. Julie Creswell and Nicole Perlroth, "Ex-Employees Say Home Depot Left Data Vulnerable," *New York Times*, September 19, 2014, http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html.

tems on Sony computers.[19] The United States publicly attributed this attack to North Korea.

- In January 2015, *Wired* magazine reported that a cyberattack on a steel mill in Germany had manipulated control systems in such a way that "a blast furnace could not be properly shut down, resulting in 'massive'—though unspecified—damage." The German government report on this incident does not specify when the attack occurred.[20]
- In February 2015, Anthem, one of the largest health insurers in the United States, announced that it had been the target of an effort to obtain the personal information of tens of millions of its customers and employees. The information in question included names, Social Security numbers, birthdays, addresses, email addresses, and employment information, including income data.[21]
- In March 2015, Premera Blue Cross, a health insurer based in Washington State, reported that the personal information of up to 11 million customers could have been exposed in a data breach that occurred in 2014.[22]
- In August 2015, the Office of Personnel Management of the U.S. government revealed that approximately 22 million personnel records of U.S. government employees—including those with high-level security clearances—had been compromised. These records contained information that went far beyond basic identifying information and, in the case of those who had applied for security clearances, included fingerprints and lists of foreign contacts.[23]

19. Lori Grisham, "Timeline: North Korea and the Sony Pictures Hack," *USA Today*, January 5, 2015, http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

20. Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, January 8, 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/. For the original German government report, see Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2014* (Bonn, 2015), http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf.

21. Reed Abelson and Matthew Goldstein, "Millions of Anthem Customers Targeted in Cyberattack," *New York Times*, February 5, 2015, http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html.

22. Jaikumar Vijayan, "Premera Hack: What Criminals Can Do with Your Healthcare Data," *Christian Science Monitor*, March 20, 2015, http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data.

23. Mike Levine and Jack Date, "22 Million Affected by OPM Hack, Officials Say," ABC News, July 9, 2015, http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731. On fingerprints, see Andrea Peterson, "OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought," *Washington Post*, September 23, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

Over time, the vast majority of instances in which cyber weapons have been used have involved the exfiltration of information—cyber exploitation—rather than an act of destruction or denial.

As for scale, few good numbers are available for the frequency with which cyber weapons have been used in the past. Part of the problem is that both failed and successful uses may easily go unreported *because they have not been noticed*. A failed penetration attempt may go unnoticed because it is unsuccessful. A successful penetration attempt may be successful precisely because it was unnoticed. Definitions of what it means to "use" a cyber weapon are also inconsistent. (For example, some analysts define use as a *successful* use, whereas others define a use as an *attempted* use, successful or not. Some analysts regard a probe to test for access points as the "use" of a cyber weapon, while others do not because such probes generally do not compromise system operation.)

With these caveats in mind, a survey by PricewaterhouseCoopers of more than 9,700 security, IT, and business executives found that respondents detected 42.8 million cybersecurity "incidents" in 2014, an increase of 48 percent over 2013.[24] A spokesman for the National Nuclear Security Agency was quoted in 2012 as saying that the agency experiences up to 10 million "security significant cyber security events" each day, of which "less than one hundredth of a percent can be categorized as successful attacks against the Nuclear Security Enterprise computing infrastructure."[25]

TODAY'S GOVERNANCE OF CYBER WEAPONS

One source refers to governance as "all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language."[26] With such a broad scope, mechanisms of governance clearly go beyond law, though law is an important aspect of governance. Governance mechanisms also include government policies, norms of behavior (which may or may not be reflected in law), codes of conduct, ethics, markets, and education. They may also involve nongovernment actors.

What aspects of cyber weapons could governance mechanisms operate or affect? In principle, three distinct aspects should be considered.

24. "The Global State of Information Security Survey 2015—Managing Cyber Risks in an Interconnected World," PricewaterhouseCoopers, n.d., http://www.pwccn.com/home/eng/rcs_info_security_2015.html.

25. Jason Koebler, "U.S. Nukes Face Up to 10 Million Cyber Attacks Daily," *U.S. News and World Report*, March 20, 2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.

26. Mark Bevir, *Governance: A Very Short Introduction* (Oxford: Oxford University Press, 2013).

- Governance might address the acquisition of some or all cyber weapons, where *acquisition* should be understood to mean research, development, testing, production, sale, transfer, or some combination thereof.
- Conceptually separate from restrictions on acquisition, governance might also seek limits on the deployment or use of some or all cyber weapons or limit the circumstances of such use.
- Lastly, governance might make use of transparency and confidence-building measures, which call for nations to take or refrain from taking certain actions in the hope that such behavior will reassure other parties about their own benign intent.

International Law Regarding Cyber Weapons

No treaties or other international agreements address any aspect of the acquisition of cyber weapons. Thus, research, development, testing, or production of cyber weapons is entirely unconstrained by international law.

In addition, no treaties or other international agreements address directly and explicitly the *use* of cyber weapons. However, some existing bodies of law may in principle be applied to the use of cyber weapons. In a 2012 speech, Harold Koh, then legal adviser to the U.S. secretary of state, explicitly stated the U.S. view that international law principles do apply in cyberspace.[27] Thus, from the U.S. perspective, international law provides an important legal framework from which to understand constraints on the use of cyber weapons.

Specifically, international law—under the rubric of the law of armed conflict (LOAC)—addresses the use of armed force by states in two ways. First, when is it legal for a nation to use force against another nation? This body of law is known as *jus ad bellum*. Second, what are the rules that govern the behavior of combatants who are engaged in armed conflict? Known as *jus in bello*, this body of law is separate and distinct from *jus ad bellum*.

The UN Charter and Jus ad bellum. *Jus ad bellum* is governed by the UN Charter (written in 1945), interpretations of the UN Charter, and some customary international law that has developed in connection with and sometimes prior to the UN Charter. Article 2(4) of the Charter prohibits nations from using "the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Article 51 provides for an exception to this prohibition, affirming the inherent right of states of self-defense in the case of an "armed attack."

The UN Charter does not formally define *use of force*, *threat of force*, or *armed attack*. Based largely on historical precedents, nations appear to agree that a variety of unfriendly actions, including unfavorable trade decisions, space-

27. See Harold Hongju Koh, "International Law in Cyberspace" (presentation at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Md., September 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm. Koh was the legal advisor of the Department of State.

based surveillance, boycotts, severance of diplomatic relations, denial of communications, espionage, economic competition or sanctions, and economic and political coercion, do not rise to the threshold of a "use of force," regardless of the scale of their effects. "Armed attack" is also likely to include declared war, occupation of territory, naval blockade, or the use of armed force against territory, military forces, or civilians abroad.

In his 2012 speech, Koh expanded on the use of cyber weapons and *jus ad bellum*, noting that:

- cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law;
- a state's inherent right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof;
- states conducting activities in cyberspace must take into account the sovereignty of other states, including outside the context of armed conflict; and
- states are legally responsible for activities undertaken through "proxy actors" who act on the state's instructions or under its direction or control.

For actions relating to security, international law also recognizes the concept of countermeasures.[28] According to Michael Schmitt, countermeasures are "State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions."[29] That is, countermeasures taken by B against A would themselves be unlawful actions were it not for the wrongful actions of A against B. B's countermeasures must be taken only for the purpose of persuading A to desist in A's wrongful actions. Moreover, countermeasures are relevant only when A's wrongful actions do not rise to the threshold of a "use of force" or "an armed attack" as the latter terms are used in the UN Charter. (If A's actions do rise to these levels, Article 2(4) and Article 51 of the UN Charter come into play.)

Countermeasures are subject to two constraints. First, they must themselves be below the threshold of a use of force or an armed attack. Second, the provoking action must be attributable to a specific responsible nation (in the example

28. In this context, *countermeasures* is a legal term that contrasts with its more technical usage. For example, in the case of biological weapons, the term *countermeasures* refers to defenses against biological warfare agents. For cyber weapons, *technical countermeasures* might refer to the use of scanners to detect malicious software or active defense measures using cyber weapons to inflict damage or pain against a cyber intruder.

29. Michael Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law* 54 (3) (2014): 697–732, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2353898.

above, A must be known to be the specific nation that is in fact responsible for the action).

The Geneva Conventions and Jus in bello. Jus in bello is governed by the Geneva Conventions of 1949 and their subsequent protocols, interpretations of the conventions, and some customary international law that has developed in connection with and sometimes prior to the conventions. Several fundamental principles underlie the Geneva Conventions, including:

- Military necessity. The only targets that may be attacked are those that make a direct contribution to the enemy's war effort or those whose damage or destruction would produce a military advantage because of their nature, location, purpose, or use.
- Proportionality. Attacks on valid military targets may result in collateral injury and damage to civilian assets or people, and thus the Geneva Conventions allow some degree of collateral damage but not if the foreseeable collateral damage is disproportionate to the military advantage likely to be gained from the attack. In the event that military and nonmilitary assets are circumstantially commingled (e.g., the use of a common electrical grid to power both military and civilian facilities), the attacker must make a proportionality judgment. If the enemy has deliberately intermingled military and nonmilitary assets or people (e.g., by using human shields), the enemy must also assume some responsibility for the collateral damage that may result. (In the latter case the attacker must still make a proportionality judgment.)
- Distinction. Distinction requires armed forces to make reasonable efforts to distinguish between military and civilian assets and between military personnel and civilians and to refrain from deliberately attacking civilians or civilian assets. The Geneva Conventions also confer special protected status on civilian facilities such as houses of religious worship and hospitals.
- Discrimination. Nations have agreed to refrain from using weapons such as biological and chemical weapons at least in part because they are inherently indiscriminate weapons. An inherently indiscriminate weapon is one that is impossible to be used in a manner that discriminates between combatants and noncombatants. However, because nearly all weapons can be *used* indiscriminately, harm to noncombatants is minimized through adherence to requirements of proportionality imposed on the use of weapons.

Regarding cyber weapons and *jus in bello*, Koh said that:

- in the context of an armed conflict, the law of armed conflict applies to regulate the use of cyber tools in hostilities, just as it does other tools;

- the *jus in bello* principle of distinction (that is, distinguishing between military and nonmilitary objectives) applies to computer network attacks undertaken in the context of an armed conflict; and
- the *jus in bello* principle of proportionality applies to computer network attacks undertaken in the context of an armed conflict.

Applying Existing International Law to the Use of Cyber Weapons. As of early 2016 no international legal precedents—no decisions by the International Court of Justice, no resolutions from the UN Security Council or General Assembly—guide interpretation of international law as it pertains to the use of cyber weapons.

A variety of reports and proposals, however, do address the topic. Perhaps the best known of these analyses—the *Tallinn Manual on the International Law Applicable to Cyber Warfare* of 2013—presents the views of twenty international law scholars and practitioners on how international law applies to cyber warfare and proposes ninety-five "black-letter rules" relevant to cyber conflict that can be derived from international law (including law related to sovereignty, state responsibility, and neutrality, as well as the UN Charter and the Geneva Conventions).[30]

Two examples of the manual's black-letter rules will give a flavor of their character:

- Rule 10 states, "A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."[31]
- Rule 37 states, "Civilian objects shall not be made the object of cyber-attacks. Computers, computer networks, and cyber infrastructure may be made the object of attack if they are military objectives."[32]

The *Tallinn Manual* was the result of an initiative undertaken by the NATO Cooperative Cyber Defence Centre of Excellence, although the book's introduction states that the manual "is not an official document but rather the product of a group of independent experts acting solely in their personal capacity."[33] The introduction further states that it does not represent the views of the Centre of Excellence, its sponsoring nations, or NATO. Nevertheless, the document is the only comprehensive source of legal analysis on this topic and is widely regarded as the most authoritative treatment to date.

30. Michael N. Schmitt et al., eds., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); hereafter "Tallinn manual." "Black-letter" rules are legal rules that are so well settled they are no longer subject to serious dispute in the legal community.

31. Ibid., 42.

32. Ibid., 124.

33. Ibid., 11.

Rule 9 of the *Tallinn Manual* briefly discusses countermeasures, stating, "A state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state."[34] The manual also notes a disagreement among its experts on what actions count as allowable countermeasures, some arguing that countermeasures entailing the use or threat of force are entirely prohibited and others arguing that a limited use of force might be appropriate if that use were below the threshold of an armed attack.

A second noteworthy document is the August 2013 report of the UN Group of Governmental Experts (GGE) on Information, Telecommunications, and International Security. This group, comprised of governmental experts on IT from fifteen nations (Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom, and the United States), was established at the request of the UN General Assembly to study "existing and potential threats in the sphere of information security and possible cooperative measures to address them including norms, rules or principles of responsible behavior of States and confidence-building measures with regard to information space, as well as the concepts aimed at strengthening the security of global information and telecommunications systems."[35]

The 2013 GGE report concludes that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technology] environment."[36] Although this statement is a recommendation of the group of experts rather than an authoritative commitment from the nations they represent, many of the experts in the group have formal affiliations with their national governments and this has frequently been interpreted as indicating a concurrence among the represented nations that international law applies to cyberspace. The report was presented to the UN General Assembly, in accordance with the report's terms of reference, after which the General Assembly unanimously took note of the report without accepting any of its specific assessments or recommendations.[37]

34. Ibid., 36.

35. "Statement by the Chair of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, H.E. Ambassador Deborah Stokes of Australia," October 25, 2013, http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_25-Oct_OWMD_Chair_UNGGE.pdf.

36. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, United Nations General Assembly, June 24, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

37. "Developments in the Field of Information and Telecommunications in the Context of International Security," A/RES/68/243, United Nations General Assembly, January 9, 2014, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/243.

In July 2015, a new UN group of government experts issued a second report on "Developments in the Field of Information and Telecommunications in the Context of International Security."[38] The new group numbered twenty and included Antigua and Barbuda, Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russia, Spain, the United Kingdom, and the United States.

Although the 2015 report does explicitly endorse other parts of the 2013 report, such as those related to capacity building, it does not explicitly endorse the conclusion of the 2013 report that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." However, Paragraph 28(c) of the 2015 report says, "Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter."[39]

Some commentators have interpreted the inclusion of Paragraph 28(c) as an implicit acknowledgment that the UN Charter applies in its entirety to the use of ICTs. Others—including this author—note that, at the very least, Paragraph 28(c) of the 2015 GGE report is nowhere as clear as the allegedly comparable statement in the 2013 report and that no nations—except the United States and the United Kingdom—have authoritatively repeated the assertion that international law applies to cyberspace.

Since the issuance of the 2015 GGE report, two significant events have occurred. In a joint statement resulting from the Sino-American summit between Presidents Xi Jinping and Barack Obama in September 2015, the two nations agreed not to "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[40] In addition, they "welcomed" the 2015 UN GGE report on cybersecurity, which recommended that states "should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[41]

Cyber-enabled theft of intellectual property has been the most significant impediment to better cyber relations between China and the United States, and

38. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, United Nations General Assembly, July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

39. Ibid.

40. White House, Office of the Press Secretary, "FACT SHEET: President Xi Jinping's State Visit to the United States," September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

41. Ibid.

the joint statement is noteworthy because China has never before made such an explicit statement on that topic. (President Xi has also issued similar joint statements with the leaders of the United Kingdom and Germany.) But observers have expressed skepticism about whether the stated commitment from China will be accompanied by an actual reduction in such theft in the future.[42] Moreover, the statement is entirely silent on the use of cyber weapons for destructive purposes against critical infrastructure.

Just two months later, the second significant event occurred when the leaders of the G20, which represents the world's largest advanced and emerging economies, agreed in the communiqué from their summit in Antalya, Turkey, that no country should conduct or support cyber theft "of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" and, further, that "we [the leaders of the G20] affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs."[43] This last statement mirrors the statement contained in the 2013 GGE report but, because it is explicitly endorsed by the national leaderships of the signatory nations, can be regarded as authoritative.

In the few months after the 2015 GGE report was released, a number of observers (including this author) were concerned that because the GGE report failed to include statements that strongly endorsed the recommendations of the 2013 report, certain nations, such as China and possibly Russia, were backing away from the 2013 statement regarding international law's applicability to cyberspace.

The G20 summit communiqué is a significant change that ameliorates some of these concerns. Whether the communiqué will be regarded as the start of an emerging consensus on cyber norms, however, remains to be seen.

The Budapest Convention. The Budapest Convention on Cybercrime of 2001 is an international agreement among forty-seven nations (including most members of the Council of Europe, the United States, Canada, Australia, and Japan).[44] Notably, Russia and China are not parties to the convention. The convention has three main purposes: to enact domestic laws that criminalize certain kinds of behavior in cyberspace; to implement certain investigative procedures

42. Even President Obama said immediately after the summit, "The question now is, 'Are words followed by actions? . . . And we will be watching carefully to make an assessment as to whether progress has been made in this area." See Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *New York Times*, September 25, 2015, http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

43. For the text of the summit communiqué, see http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-pdf/. The G20 members are Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the United Kingdom, the United States, and the European Union.

44. "Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime," Council of Europe, updated February 11, 2016, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

for law enforcement in the signatory nations; and to enhance international cooperation regarding law enforcement activities against cybercrime.[45]

- Criminalized behavior. Some of the behaviors that parties to the convention agree to criminalize include improper access to a computer, improper interception of data, data interference, system interference, and misuse of devices.[46] In many cases, the use of a cyber weapon could be included under these rubrics.
- Investigatory procedures. Parties to the convention agree to enact a variety of procedural mechanisms and procedures to facilitate the investigation of cybercrimes or any crimes committed with a computer or for which evidence may be found in electronic form.
- International cooperation. Parties to the convention agree to implement mechanisms through which they will assist one another in investigating cybercrimes and other crimes involving electronic evidence. However, cooperation may be limited or delayed by a nation's domestic laws or by other arrangements. In addition, parties can usually decline to cooperate if such cooperation would compromise their sovereignty, security, law enforcement, public order, or other essential interests.

Of these purposes, only the first category addresses the governance of cyber weapons as such—focusing on uses of cyber weapons that should be discouraged through criminalization.

The Budapest Convention itself does not establish international law that criminalizes specific behaviors. Rather, it harmonizes domestic criminal law across the signatory nations regarding these behaviors.

The Agreement between the Member States of the Shanghai Cooperation Organization. In June 2009, the six member states of the Shanghai Cooperation Organization (Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan) concluded a Russian-drafted agreement defining "information wars" broadly as a "confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, critical and other structures, undermining political, economic and social systems, [and] mass psychologic brainwashing to destabilize society and state."[47] While

45. The discussion of the Budapest Convention is based largely on Michael Vatis, "The Council of Europe Convention on Cybercrime," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010).

46. The text of the convention refers to access and interception "without right," a term that means "without proper legal authorization."

47. "Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security, Yekaterinburg, 16 June 2009," in S. A. Komov, ed., *International Information Security: The Diplomacy of Peace—Compilation of Publications and Documents* (Moscow, 2009), 202–213. This is an unofficial translation; the authentic languages of the Agreement are Russian and Chinese.

this definition does include cyberattack within its ambit, the status of cyber exploitation is uncertain.

For the most part, this agreement was a joint statement among the signatories emphasizing their views on the undesirability of information war. However, Article 4(1) states, "The parties shall cooperate and act in the international information space within the framework of this agreement in such a way that the activities contribute to social and economic development and comply with maintaining international security and stability, generally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms and the principles of regional cooperation and non-interference in the information resources of the States of the Parties."

In the reading of this author, this statement does not require any signatory to refrain from any particular action in cyberspace. The agreement commits the parties to take actions that contribute to social and economic development in a manner consistent with the principles listed, but it does not explicitly prohibit one signatory from launching cyberattacks against another if, in the judgment of the launching nation, such attacks might help to maintain security and stability.

The Sino-Russian Cyber Security Agreement of 2015. On May 8, 2015, the Russian Federation and the People's Republic of China signed an agreement to cooperate on information security,[48] a term that is discussed in greater detail in a later section of this paper. Article 4(3) states, "Each Party has an equal right to the protection of the information resources of their state against misuse and unsanctioned interference, including computer attacks against them. Each Party shall not exercise such actions with respect to the other Party and shall assist the other Party in the realization of said right."[49] Dr. Elaine Korzak, at the time of this writing a National Fellow at the Hoover Institution of Stanford University, notes that these two sentences together could be read in a way to prohibit Russia and China from using "computer attacks" against each other.

A Note on Cyber Espionage. The term *cyber weapon* encompasses all applications of IT that have an impact on the integrity, availability, or confidentiality of information inside a targeted information system or network, being carried through it, or being processed within it. This definition focuses on the technical dimensions of cyber weapons, but the *legal* distinction between these kinds of impact is significant.

48. Andrew Roth, "Russia and China Sign Cooperation Pacts," *New York Times*, May 8, 2015, http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html. For the original, Russian-language version of the Russian-Chinese agreement, see http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf. For an unofficial English-language translation, see James Lewis, "Sino-Russian Cybersecurity Agreement 2015," CSI Strategic Technologies Program, May 11, 2015, http://www.csistech.org/blog/2015/5/11/sino-russian-cybersecurity-agreement-2015.

49. Elaine Korzak, "The Next Level for Russia-China Cyberspace Cooperation?" *Net Politics* (blog), Council on Foreign Relations, August 20, 2015, http://blogs.cfr.org/cyber/2015/08/20/the-next-level-for-russia-china-cyberspace-cooperation/.

In particular, compromises of *confidentiality* are usually regarded as espionage. Most important, a compromise of confidentiality still leaves the targeted computer working exactly as it did before—if I steal a $10 bill from you, I have it and you do not. But if I steal your Social Security number, I have it and you still have it. Espionage—whether committed through cyber or noncyber means—is illegal under the domestic laws of virtually all nations, but it is not forbidden under international law. For example, W. Hays Parks (former Defense Department attorney and Special Assistant to the Army Judge Advocate General) writes,

> Each nation endeavors to deny intelligence gathering within its territory through domestic laws . . . . Prosecution under domestic law (or the threat thereof) constitutes a form of denial of information rather than the assertion of a *per se* violation of international law; domestic laws are promulgated in such a way to deny foreign intelligence collection efforts within a nation's territory without inhibiting that nation's efforts to collect intelligence about other nations. No serious proposal has ever been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each.[50]

Thus, by this logic, espionage conducted by or through the use of a computer—also known as cyber espionage—is also not forbidden by international law, and nations that engage in cyber espionage do derive significant benefit from it.

U.S. Domestic Law Regarding Cyber Weapons

In the United States, no domestic law addresses any aspect of research, development, testing, or production of cyber weapons. However, the United States criminalizes unauthorized access to computers under the Computer Fraud and Abuse Act (CFAA). Most significant, the CFAA criminalizes unauthorized access originating from any party under U.S. jurisdiction to any computer connected to the Internet, wherever in the world the computer is located. That access may be effected in any number of ways, including through the use of a cyber weapon. The CFAA contains an explicit exception for U.S. law enforcement and intelligence agencies, however, allowing them to engage in activities that are otherwise prohibited under the act.

The United States also criminalizes unauthorized interception of electronic communications under the provisions of the Electronic Communications Privacy Act (ECPA), as amended. (The ECPA also contains a number of exceptions applying to U.S. law enforcement and intelligence agencies.) Under the defini-

50. W. Hays Parks, "The International Law of Intelligence Collection," in *National Security Law*, ed. John Norton Moore and Robert Turner (Durham, NC: Carolina Academic Press, 1990), 433–434.

tions used in this chapter, an application of IT that enabled the interception of communications would be classified as a cyber weapon.

Many domestic laws criminalize actions without specific regard for the instruments used in those actions. For example, the Economic Espionage Act criminalizes the stealing of economic information but does not specifically mention how one might effect such a theft. Today such theft is often perpetrated through the use of cyber weapons.

As for domestic law regarding the export of cyber weapons, the United States is a party to the Wassenaar Arrangement, in which a number of states have agreed to regulate exports of certain cyber weapons and related dual-use technologies. (In this case, the adopted definition of *dual-use technologies*—namely, technologies that can be used for either civilian or military purposes—is that of the U.S. government.) This arrangement was established "to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities."[51] In the United States, controlled dual-use technologies are enumerated on the Commerce Control List (CCL),[52] and the export of items on the CCL is administered by the Department of Commerce.

For many years, certain technologies for cyber defense were controlled in this manner. Restricting the availability of these technologies to undesirable nations made attacking or conducting signals intelligence against them easier. But in March 2014, certain technologies for cyber weapons were added to the Wassenaar control list.[53]

- Under Category 4-A-5: "Systems, equipment, and components therefor, specially designed or modified for the generation, operation, or delivery of, or communication with, 'intrusion software'"—where "intrusion software" is "'Software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network-capable device, and performing any of the following: (a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; *or* (b) The modification of the standard execution path of a

51. "About Us," n.d., http://www.wassenaar.org/introduction/index.html.

52. https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

53. *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: List of Dual-Use Goods and Technologies and Munitions List* (Vienna: Wassenaar Arrangement, 2014), http://www.wassenaar.org/wp-content/uploads/2015/07/WA-LIST-14-2.pdf.

program or process in order to allow the execution of externally provided instructions."[54]

- Under Category 5-A-1-j: "IP network communications surveillance systems or equipment, and specially designed components therefor" with certain technical capabilities.[55]

A particular twist to the Wassenaar formulation is that it apparently applies controls not to a hostile payload but to the means of delivery and creation of hostile payloads. That is, the payload per se—the part of a cyber weapon that actually causes negative effects on the targeted computer—is unaffected by the Wassenaar Arrangement.[56] Thus, a destructive payload could be exported freely as long as it was not packaged with a penetration mechanism. The reason for this exception is unknown.

As an example of the Wassenaar Arrangement's impact, VUPEN Security, a leading seller of vulnerabilities, changed its sales policy to sell its products only to approved government agencies in approved countries. VUPEN also announced it would automatically exclude countries subject to European Union restrictions and countries subject to embargoes by the United States or the UN.[57]

The Wassenaar Arrangement is a harmonization regime for the domestic laws of its signatories rather than an international legal agreement. In this regard it is similar to the Budapest Convention.

Export Controls on Munitions

Export controls have long been used to stem the proliferation of certain "dangerous" technologies; that is, technologies that would be dangerous were they to fall into the hands of adversaries. In the United States, the Arms Export Control Act of 1976 (22 USC 39) gives the president authority to control the export of defense articles and defense services. (Defense articles and services are those intended explicitly and primarily for military use and thus do not fall into the "dual-use" category.) The act is implemented by the International Traffic in Arms Regulations (ITAR), and the regulated defense articles and services are found on the United States Munitions List (USML).[58] The Department of State administers the ITAR.

54. Ibid., 73, 212.

55. Ibid., 81.

56. For more discussion of the application of export controls to different components of a cyber weapon, see Trey Herr and Paul Rosenzweig, "Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model," *Journal of National Security Law and Policy* 8 (2) (2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2501789.

57. Jennifer Granick and Mailyn Fidler, "Changes to Export Control Arrangement Apply to Computer Exploits and More," *Just Security*, January 15, 2014, http://justsecurity.org/5703/export-control-arrangement-apply-computer-exploits/.

58. For the USML, see 22 CFR 121, https://www.pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf.

Information technologies found on the munitions list are mostly found in Category XIII (auxiliary military equipment) and include military information, security assurance systems and equipment, cryptographic devices, software, and components specifically designed, developed, modified, adapted, or configured for military applications (including command, control, and intelligence applications). Items 1, 2, and 4 of this list contain defensive cyber technologies that the United States would prefer to keep out of the hands of adversaries; doing so enables the United States to conduct more effective attacks or espionage in cyberspace. Item 3 on the list contains the only mention of technology related to cyber weapons: military cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components, or software that would enhance an adversary's signals intelligence capabilities.

However, Category 21 (miscellaneous items) of the Wassenaar Arrangement is a catchall category for items not enumerated in the other categories: "Any article not specifically enumerated in the other categories of the U.S. Munitions List which has substantial military applicability and which has been specifically designed, developed, configured, adapted, or modified for military purposes. The decision on whether any article may be included in this category shall be made by the Director, Office of Defense Trade Controls Policy." Authorities related to Category 21 are not likely to have been used to restrict the transfer of cyber weapons to other nations.[59]

The original purpose of ITAR and the USML was to regulate the sale of weapons designed and intended for military purposes. But IT is inherently dual-use, and thus a clear definition of when an IT artifact with some destructive or damaging capability is designed or intended for *military* purposes is elusive. Recognizing a military purpose for an IT artifact that is also used in a civilian context is problematic. Thus, judgments about the permissibility of a U.S. sale of cyber weapons to Nation X will, more likely than not, be based less on the capabilities of the artifacts involved and more on the perceived intentions of Nation X and the U.S. relationship with Nation X.

U.S. Policy Statements Concerning Cyber Weapons

In May 2011 the White House released its *International Strategy for Cyberspace*. This document was remarkable for its near-total silence regarding the acquisition or use of cyber weapons. The closest the document comes to this topic is its statement that, "consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace." It further states, "the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. . . . We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests." Nevertheless, the document emphasizes, "we will exhaust all options before military force

59. Trey Herr, George Washington University, personal communication, September 2015.

whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible."[60]

The document also speaks of norms of behavior that its authors believe could bring "predictability to state conduct, helping prevent the misunderstandings that could lead to conflict." In addition to the right of self-defense as one such norm, the document argues, "States must identify and prosecute cybercriminals [presumable criminals using cyber weapons], to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner."[61] (Compliance with such norms during conflict is not—and cannot be—assured.)

Another policy statement was made by Michael Daniel, special assistant to the president and White House cybersecurity coordinator, in an April 2014 blog post. In this post, Daniel discusses the tension between revealing a vulnerability in a system so that it can be repaired (thus improving security for those using that system) and withholding knowledge of that vulnerability (thus enabling those with that knowledge, such as the U.S. government, to use that vulnerability as part of a cyber weapon). He further noted that when the U.S. government does obtain knowledge of such a vulnerability, the administration "takes seriously its commitment to an open and interoperable, secure and reliable Internet, and in the majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. This has been and continues to be the case."[62] To the extent that this is actually the case (there is significant public skepticism on this point), disclosure helps to inhibit the development of cyber weapons.

In April 2015, the DOD released *The DOD Cyber Strategy*.[63] This document went further than any previous official statement in asserting the right of the United States to use cyber weapons. Three passages in the document warrant special attention.

60. White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: White House, May 2011), 10, 14, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

61. Ibid., 9–10.

62. Michael Daniel, "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities," *White House Blog*, April 28, 2014, https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

63. Department of Defense, *The DOD Cyber Strategy* (Washington, D.C.: DOD, April 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

- "There may be times when the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military-related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyber operations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests. United States Cyber Command (USCYBERCOM) may also be directed to conduct cyber operations, in coordination with other U.S. government agencies as appropriate, to deter or defeat strategic threats in other domains."[64]
- "[A strategic goal of the DOD cyber strategy is to] build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages. During heightened tensions or outright hostilities, DOD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, DOD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities. . . . To ensure unity of effort, DOD will enable combatant commands to plan and synchronize cyber operations with kinetic operations across all domains of military operations."[65]
- "DOD will work with agencies of the U.S. government as well as U.S. allies and partners to integrate cyber options into combatant command planning."[66]

The United States thus reserves the right to use cyber weapons to militarily protect U.S. interests in an area of operations, to deter or defeat strategic threats in other domains, and to integrate the use of cyber weapons into military planning efforts as an additional tool, albeit with special characteristics, in the U.S. arsenal.

Around the same time, in May 2015 in Seoul, Secretary of State John Kerry delivered a speech on the Internet. After reiterating the U.S. view that the basic rules of international law apply in cyberspace, that acts of aggression are not permissible, and that countries that are hurt by a cyberattack have a right to respond in accordance with the laws of armed conflict, he said that the United States also "support[s] a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace."[67]

64. Ibid., 5.

65. Ibid., 14.

66. Ibid., 26.

67. "Text of John Kerry's Remarks in Seoul on Open and Secure Internet," Voice of America, May 18, 2015, http://www.voanews.com/content/text-of-john-kerrys-remarks-in-seoul-on-open-and-secure-internet/2776139.html.

He did not use the term *norms* in this context, but Kerry's principles are in fact norms by any conventional definition of the term. These principles include the following (with the author's principle-by-principle commentary indented and in brackets after each quotation from Kerry's speech):

- "No country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure."

  [This principle can be construed as limiting the use of cyber weapons against another nation's critical infrastructure. (Other analysts have suggested restrictions on targeting critical infrastructure as well.[68]) Such restrictions would be in some ways analogous to prohibitions on targeting hospitals and places of worship as provided by the Geneva Conventions. However, the Kerry speech does not define critical infrastructure, and in the United States, at least, a large fraction of the U.S. economy (well over 50 percent) is categorized as such. The principle is also silent about the extent of damage or impediment that it forbids. At the upper end (a large-scale cyberattack against critical infrastructure that results in nationwide collapse of that infrastructure), LOAC already rules out such an attack because it would be likely to result in a large amount of damage and harm to civilians and thus to fail the LOAC test of proportionality. At the lower end (e.g., a small cyberattack against a single electrical generator powering a military facility), it is hard to imagine that the principle is intended to prohibit such an action. Indeed, *The DOD Cyber Strategy* explicitly says that military-related critical infrastructure is *not* off-limits. Lastly, agreements to refrain from such targeting can remove an overt and openly declared cyber threat against these facilities, but all of the concerns about actual attacks on these facilities will continue to be unaddressed, a point that has two consequences: (1) The cyber defenses of critical infrastructure must be just as strong and robust as they would be in the absence of a targeting agreement. That is, the defense of critical infrastructure is not simplified or made easier in any way by such an agreement. (2) Political costs that might be expected to accrue to a violator of such an agreement could be mitigated to some degree by the inherent plausible deniability of cyber operations. Political costs accrue only if evidence is available that would convince

68. "Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security," Atlantic Council, November 5, 2014, http://www.atlanticcouncil.org/publications/reports/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security; and John Steinbruner, "Prospects for Global Restraints on Cyberattack," *Arms Control Today* 41 (December 2011), http://legacy.armscontrol.org/act/2011_12/Prospects_for_Global_Restraints_on_Cyberattack.

third-party observers of responsibility in the face of outright denial by the perpetrator, and finding convincing evidence is particularly problematic in the cyber world.]

- "No country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm."

  [This principle can be construed as limiting the use of cyber weapons against computer emergency response teams and is somewhat analogous to restrictions on targeting hospitals, medical personnel, or ambulances.]

- "No country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain."

  [This principle is limited to prohibiting the obtaining of data for commercial gain but leaves unrestricted the obtaining of data for purposes related to national security. As such, this principle places no restrictions on the actual use of cyber weapons per se, though it does restrict the purposes to which the results of such use may be put.]

- "Every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way."

  [This principle is silent on the use of cyber weapons per se, though it seeks to assign state responsibility for suppression of such use.]

- "Every country should do what it can to help states that are victimized by a cyberattack."

  [This principle is silent on the use of cyber weapons.]

Lastly, the U.S. Congress expressed concerns about the proliferation of cyber weapons in Section 940 of the National Defense Authorization Act for Fiscal Year 2014, which required the president to "establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate."[69]

According to the legislation, this policy was to have two purposes:

- To identify the intelligence, law enforcement, and financial sanctions tools that can and should be used to suppress the trade in cyber tools and infrastructure that are or can be used for criminal, terrorist, or military activities while preserving the ability of governments and the private sector to use such tools for self-defense.

69. https://www.gpo.gov/fdsys/pkg/CPRT-113HPRT86280/pdf/CPRT-113HPRT86280.pdf.

- To establish a statement of principles to control the proliferation of cyber weapons, including principles for controlling the proliferation of cyber weapons that can lead to expanded cooperation and engagement with international partners.

As of April 2016, the administration had not produced the requested report. Further, whether the concerns of Congress were related to cyber weapons as mostly military artifacts or as dual-use artifacts is not clear. Supporting the former interpretation is the fact that the legislation passed as a part of the DOD authorization bill; supporting the latter interpretation is the idea that government and private sector entities had legitimate interests in cyber weapons for self-defense purposes.

Existing Transparency and Confidence-Building Measures

Confidence-building measures (CBMs) are measures that two or more nations agree to take to reduce the likelihood that a conflict might break out between or among them because of miscalculation or misperception or that a conflict might inadvertently escalate. As far as is known to this author, only one specific and currently extant CBM relates to cyberspace. At talks during the G-8 meeting in June 2013, the United States and the Russian Federation agreed on CBMs for cyberspace to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis.[70] The measures include:

- The establishment of a direct secure voice communications line between the U.S. Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council, should there be a need to directly manage a crisis situation arising from a cybersecurity incident. It is planned that this direct line will be seamlessly integrated into the existing Direct Secure Communication System ("hotline") that both governments already maintain.
- The establishment of secure and reliable lines of communication for each nation to make formal inquiries of the other about cybersecurity incidents of national concern so as to reduce the possibility of misperception and escalation from cybersecurity incidents. The existing Nuclear Risk Reduction Center links established in 1987 between the two nations will house these cyber lines of communication.
- The sharing of threat indicators between the United States Computer Emergency Readiness Team and its counterpart in Russia, including technical information about malicious software or other indicators reflecting malicious activity appearing to originate from each other's territory. Sharing such information helps in the proactive mitigation of threats.

70. White House, Office of the Press Secretary, "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security," June 17, 2013, http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

Nothing in this arrangement speaks directly to governing either the acquisition or use of cyber weapons (or the underlying technology).

Current State of Governance of Cyber Weapons in Other Countries

Many states other than the United States criminalize unauthorized access to computers (see, for example, the UK's Computer Misuse Act 1990).[71] However, to the best of this author's knowledge, no state has attempted to regulate the *acquisition* of cyber weapons within its borders.

A number of states also place export controls on technologies relevant to cyber weapons, thus limiting the acquisition of cyber weapons by certain nations. In some cases, these controls closely mirror the U.S. controls (for example, when the nations in question are parties to the Wassenaar Arrangement); in others they are somewhat different.

Outside the United States, the government of the Netherlands has been comparatively outspoken in its discussion of offensive operations in cyberspace. For example, in December 2009, some members of the Dutch Parliament stated that defensive capabilities alone were insufficient to engage in cyber warfare.[72] In December 2011, an advisory committee to the Dutch government freely discussed the value of using cyber weapons (under the rubric of *offensive cyber capabilities* as a rough synonym for *cyber weapons*).[73] For example, it endorsed the view that such weapons could be used to protect friendly systems and networks. In January 2012, the Dutch government stated that its Ministry of Defence was investing in measures to develop "new (including offensive) [cyber] capabilities."[74] And in February 2015, the Dutch minister of defense released a six-page letter that revises the Dutch Defense Cyber Strategy of 2012.[75] This letter identifies as priorities the "strengthening [of] the intelligence capability in the digital domain" and "strengthening the use of cyber in military missions,"

71."Computer Misuse Act 1990," n.d., http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences.

72. "Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2010," Vergaderjaar 2009–2010, Kamerstuk 32123-X nr. 66, December 10, 2009, https://zoek.officielebekendmakingen.nl/kst-32123-X-66.html.

73. Advisory Council on International Affairs (AIV) and Advisory Committee on Issues of Public International Law (CAVV), *Cyber Warfare*, AIV no. 77 / CAVV no. 22 (The Hague: AIV and CAVV, December 2011), http://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf.

74. "Government Response to the AIV/CAVV Report on Cyber Warfare," Rijksoverheid, April 26, 2012, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf.

75. "Defensie Cyber Strategie," Tweede Kamer der Staten-Generaal, Vergaderjaar 2014–2015, 33 321, nr. 5, http://www.tweedekamer.nl/downloads/document?id=194c5e2b-c5c0-4691-9d85-51f4ba38b094&title=Actualisering%20Defensie%20Cyber%20Strategie%20.docx. For an unofficial translation of this letter, see "Dutch Defense Cyber Strategy—Revised February 2015," *Matthijs R. Koot's Notebook* (blog), February 23, 2015, https://blog.cyberwar.nl/2015/02/dutch-defense-cyber-strategy-revised-february-2015/.

and the discussion of both priorities includes explicit mention of the role that offensive cyber capabilities play in supporting them.

Also, the government of the United Kingdom said in September 2013 that it is "developing a full spectrum military cyber capability, including a strike capability."[76] The UK government has not officially provided any details on this point, although Defence Secretary Philip Hammond said in an interview with the *Daily Mail* that "clinical 'cyber strikes' could disable enemy communications, nuclear and chemical weapons, planes, ships and other hardware."[77]

OTHER PROPOSALS FOR MANAGING THE RISKS FROM CYBER WEAPONS

State Initiatives at the United Nations[78]

The vast majority of cybersecurity discussions at the UN have taken place under the auspices of the various committees of the General Assembly, primarily the First Committee (whose mandate is to focus on disarmament and international security). In 1998, the Russian Federation introduced a draft resolution to the First Committee entitled "Developments in the Field of Information and Telecommunications in the Context of International Security."

The draft resolution invited interested states to submit their views on the topic, and the Russian submission stated that work should begin on the development of international principles that would "subsequently be incorporated into a multilateral international legal instrument" to regulate "information weapons." In its letter initiating deliberations in the First Committee, the Russian Federation wrote of "the creation of information weapons and the threat of information wars, which we understand as actions taken by one country to damage the information resources and systems of another country."[79]

The Russian Federation was the sole sponsor of draft resolutions with the same name until 2006, at which time China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan joined Russia as cosponsors.

76. Ministry of Defence, Joint Forces Command, and Philip Hammond, "New Cyber Reserve Unit Created," GOV.UK, September 29, 2013, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit.

77. Simon Walters, "Hammond's £500m New Cyber Army," *Daily Mail*, September 28, 2013, http://www.dailymail.co.uk/news/article-2436946/Hammonds-500m-new-cyber-army-As-reveals-secret-Whitehall-bunker-time-Defence-Secretary-says-future-wars-fought-viruses.html.

78. The discussion of initiatives at the UN borrows freely from Elaine Korzak, "Computer Network Attacks and International Law" (PhD dissertation, King's College London, 2014).

79. "Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General," A/C.1/53/3, United Nations General Assembly, September 30, 1998, https://disarmament-library.un.org/UNODA/Library.nsf/1c90cfa42bbb0d6985257631004ff541/663e6453bdaa2e228525765000550277/$FILE/A-C1-53-3_russia.pdf.

On a parallel but related track, China, Russia, Tajikistan, and Uzbekistan jointly presented in September 2011 to the UN General Assembly a proposal for an international code of conduct for information security.[80] An updated version of this proposal was presented in January 2015. According to the updated version, the purpose of the code is to "ensure that the use of information and communications technologies and information and communications networks facilitates the comprehensive economic and social development and well-being of peoples, and does not run counter to the objective of ensuring international peace and security."[81]

The most significant part of the proposed code related to dual-use is the obligation of signatories "not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security."[82]

Proposals for Confidence-Building Measures and Norms of Behavior

One set of CBMs was proposed by the Organization for Security and Co-operation in Europe in 2013 with the purpose of reducing "the risks of misperception, escalation, and conflict that may stem from the use of ICTs."[83]

- Measure 3 of the proposed set of CBMs calls for participating states to engage in "consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICT." This measure acknowledges the possibility that the use of cyber weapons could under some circumstances lead to tension or conflict. A hypothetical example of such a possibility, not mentioned in the report, is the use of cyber means by Nation A to gather intelligence information during a crisis involving A and Nation B. Such an action by A, taken with the best of intentions (e.g., to understand B's intentions during the crisis), may well be interpreted by B as a prelude to attack.
- Measure 8 calls on states to "establish measures to ensure rapid communication at policy levels of authority to permit concerns to be raised at the national security level." This measure is essentially a mechanism for greater communication during crisis.

In addition, the GGE report of 2013 was charged with studying CBMs to address existing and potential threats to information security. But a careful

80. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf.

81. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf.

82. Ibid.

83. http://www.osce.org/pc/109168?download=true.

examination of the report reveals only three statements that can even remotely be related to the governance of cyber weapons.[84]

- Paragraph 22 says, "States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies." Criminal or terrorist use of ICTs would count as use of cyber weapons, but the paragraph presents no specifics about the kind(s) of use that should be criminalized. This paragraph seems to be urging states toward the Budapest Convention or a similar arrangement.
- Paragraph 23 says, "States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs." The language about proxies suggests the undesirability of a nation "outsourcing" the use of cyber weapons to a third party (a proxy), which could in principle be a nonstate actor. The third sentence asks states to assume the responsibility of suppressing the illegal use of cyber weapons from their territories. But since *government* use of cyber weapons is likely to be legal under the laws of the using nation, the third sentence is silent on such use.
- Paragraph 26(f) says, "Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security." This language acknowledges that certain criminal acts involving the use of cyber weapons could be interpreted as hostile actions and suggests that more law enforcement cooperation between nations could help to reduce the likelihood of misinterpretation.

The GGE report of July 2015 offers recommendations regarding "voluntary, non-binding norms, rules, or principles for the responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment."[85] These recommendations include the following (with the author's recommendation-by-recommendation commentary indented and in brackets):

- Paragraph 13(f) indicates, "A State should not conduct or knowingly support ICT activity . . . that intentionally damages critical infrastructure

84. "Statement by the Chair of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, H.E. Ambassador Deborah Stokes of Australia," October 25, 2013, http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_25-Oct_OWMD_Chair_UNGGE.pdf.

85. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, 7.

or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[86]

[As with the first principle identified in Secretary of State Kerry's May 2015 speech, the language does not provide a definition of critical infrastructure; it is also silent on the question of extent of damage that would be involved in a proscribed act, a silence that almost certainly reflects differing interpretations of what this norm would mean in practice.]

- Paragraph 13(i) indicates, "States should take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products."[87]

  [This recommendation speaks to the possibility that cyberattacks might originate in or depend on compromises in the supply chain of IT products or services, but it is otherwise silent on the matter.]

- Paragraph 13(k) indicates, "States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams . . . [nor] use authorized emergency response teams to engage in malicious international activity."[88]

  [As with the second principle identified in Secretary of State Kerry's May 2015 speech, this norm can be construed as limiting the use of cyber weapons against computer emergency response teams, and it is somewhat analogous to restrictions on targeting hospitals, medical personnel, or ambulances.]

Norms and CBM proposals focusing on the use of cyber weapons and related issues originating from other analysts include:

- Measures to improve crisis management, such as hotlines that enable direct communications between states during a cyber crisis and the sharing of threat information.[89] (The United States and Russia established a means for direct communication in 2013.) Greater communication among responsible authorities during a crisis may be helpful to the extent that the content of these communications are believable. But

86. Ibid., 8.

87. Ibid.

88. Ibid.

89. Katharina Ziolkowski, *Confidence Building Measures for Cyberspace—Legal Implications* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), https://ccdcoe.org/publications/CBMs.pdf; "Cyber Security," North Atlantic Treaty Organization, updated February 10, 2016, http://www.nato.int/cps/en/natohq/topics_78170.htm; ABIresearch and International Telecommunication Union, *Global Cybersecurity Index: Conceptual Framework* (Geneva: ITU, n.d.), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf; and "Cybersecurity Information Exchange Techniques (CYBEX)," International Telecommunication Union, n.d., http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybex.aspx.

given the fact that the successful use of cyber weapons depends entirely on stealth and deception, participants in these communications may well have cause for skepticism about what the other side is saying. An additional concern is that, as with all CBMs, some degree of political will is necessary for their successful operation. A case in point is the military hotline between the United States and China. Intended to enable direct communication between senior military leaders on both sides during a crisis, it has not always been operational even during routine tests of the system. On several occasions in which the line was tested for operational capability, as well as in the wake of the 2001 EP-3 incident over Hainan Island,[90] the Chinese military failed to respond.[91]

- Bans on distributed denial of service (DDOS) attacks.[92] DDOS attacks are among the most frequent attacks on cyber infrastructure, and while they continue, they can be crippling to the targeted organization. On the other hand and in contrast to permanently destructive action, their effects are temporary and reversible—after they stop, the targeted organization is as good as new. But the most significant point regarding DDOS attacks is that powerful DDOS attacks can be launched by nonstate actors, and constraining the actions of such parties continues to be problematic. Even worse, if such attacks by nonstate actors do occur, suspicious targeted nation-states might still be inclined to blame other nations for violating the bans in question.

Many CBMs were originally developed to address issues arising in the context of kinetic armed conflict. As such, they presumed the existence of easily observed physical entities (soldiers, tracked and wheeled vehicles, artillery pieces, ships, airplanes, missiles). Movements of these entities from one geographic region to another had bearing on what they might or might not be able to do in a conflict. The number of physical entities was an important contributor to military power and capability.

90. In the EP-3 incident over Hainan Island in the South China Sea, a U.S. EP-3 reconnaissance plane collided with a Chinese F-8 fighter. The Chinese pilot died in the incident and the EP-3 made an emergency landing of the damaged plane onto Hainan Island. Given the involvement of both U.S. and Chinese military forces in this incident, U.S. military leaders tried to contact their counterparts in China to resolve the situation without undue escalation. Congressional Research Service, *China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications, October 10, 2001*, available at https://www.fas.org/sgp/crs/row/RL30946.pdf.

91. Michael D. Swaine, Tuosheng Zhang, and Danielle Cohen, eds., *Managing Sino-American Crises: Case Studies and Analysis* (Baltimore: Johns Hopkins University Press, 2006); James A. Lewis, CSIS, personal communication, September 2014; and Adam Segal, Council on Foreign Relations, personal communication, July 2015.

92. Robert K. Knake, Internet Governance in an Age of Cyber Insecurity, Council Special Report no. 56 (Washington, D.C.: Council on Foreign Relations, September 2010), http://www.cfr.org/internet-policy/internet-governance-age-cyber-insecurity/p22832. A DDOS attack is one in which many different compromised computers send bogus service requests to a single target, which is overwhelmed trying to service these (fake) requests and is thus unable to provide service for legitimate users of the targeted system.

Cyberspace is very different. For example, physical distance has little meaning in cyberspace. Forces as such do not move from one area to another. The key weaponry in cyber conflict is usually software—digitized information—and as such is intangible. Along with other fundamental differences, such as the availability of many cyber weapons to nonstate entities, measures that take for granted the unique characteristics of cyber weapons are unlikely to be useful in reducing the likelihood of cyber conflict.

Policy Proposals from the Information Technology Industry

The IT industry is an important stakeholder in the emergence of behavioral norms around the use of cyber weapons. Of particular note is a proposal from Microsoft for six norms intended to guide the behavior of nation-states with respect to the use of cyber weapons and to reduce the risk arising from such use.

- Norm 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
- Norm 2: States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
- Norm 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
- Norm 4: States should commit to nonproliferation activities related to cyber weapons.
- Norm 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.
- Norm 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.[93]

The intent behind these norms of behavior is to minimize state actions that compromise the trust of users in the products and services that private sector IT vendors offer. From the standpoint of these vendors, the economic rationale for the norms, particularly norms 1 and 2, is clear: actions that undermine public trust in IT products and services make the public more reluctant to use those products and services, an outcome with foreseeable negative economic consequences. Furthermore, to the extent that national security (e.g., of the United States) is tied to a thriving and vibrant IT industry, national security would benefit as well from widespread adoption of these norms.

93. Microsoft Corporation, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* (Redmond, WA: Microsoft Corporation, December 2014), 11–13, http://aka.ms/cybernorms.

Observing these norms of behavior would not prohibit the use of all cyber weapons—only those that are based on taking advantage of design or implementation vulnerabilities existing in deployed products and services. In principle, the use of other cyber weapons—such as those based on taking advantage of flawed configurations (e.g., a port left open when it should have been closed) or taking advantage of features designed into the product or service in an unexpected or novel way—would still be allowable. Denial of service attacks would also be permissible in principle as well, as long as the computers used to launch such attacks had not been compromised through a design or implementation vulnerability. But these norms would inhibit "zero-day" penetrations or compromises (which are regarded as being enormously powerful) and would unambiguously commit nations to help vendors improve the security of the products and services they offer.

A second step the private sector—specifically vendors of IT products and services—has begun to take is to reduce the number of vulnerabilities through "bug bounty" programs. A bug bounty program is an offer from a vendor to pay and otherwise recognize individuals who report vulnerabilities in the product or services of that vendor. A continuously updated list of such programs is maintained online.[94] When these programs work, they provide vendors with information about previously unknown vulnerabilities that they can then repair before adversaries can take advantage of them. In addition, at least one firm has been established with a business model that connects finders of vulnerabilities with the appropriate bug bounty programs.[95]

By reducing the number of unknown vulnerabilities available to developers of cyber weapons, bug bounty programs are in principle a market-based mechanism that helps to inhibit the development of such weapons. However, the extent to which these programs have been successful in doing so is not yet known.

The Role of Scientists, Scientific Societies, and Community Norms

The major society in the United States associated with computer professionals is ACM (formerly the Association for Computing Machinery). ACM includes about one hundred thousand members, which is only a small fraction of the number of programmers and software developers in the United States.[96] Membership is available to anyone for a nominal fee, and the major benefit of membership is access to an array of professional journals.

94. "The Bug Bounty List," Bugcrowd, n.d., https://bugcrowd.com/list-of-bug-bounty-programs.

95. Nicole Perlroth, "HackerOne Connects Hackers with Companies, and Hopes for a Win-Win," *New York Times*, June 7, 2015, http://www.nytimes.com/2015/06/08/technology/hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html.

96. Abel Avram, "IDC Study: How Many Software Developers Are Out There?" *InfoQ*, January 31, 2014, http://www.infoq.com/news/2014/01/IDC-software-developers; and Bureau of Labor Statistics, "Software Developers," *Occupational Outlook Handbook*, n.d., http://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm.

ACM promulgates a code of ethics for its members, of which two provisions are relevant. Section 1.2 requires members to "avoid harm to others" and prohibits "use of computing technology in ways that result in harm. . . . Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources." Section 2.8 requires members to "access computing and communication resources only when authorized to do so" and states that "one must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time."[97]

The code is silent about the responsibility of members to refrain from *creating* or *developing* cyber weapons; it speaks only to use.

On the educational side, accreditation of university-level computer science programs is provided by the Computer Science Accreditation Board, a member of the Accreditation Board for Engineering and Technology (ABET), a nonprofit, nongovernmental organization that accredits over 3,400 programs at nearly seven hundred colleges and universities in twenty-eight countries.[98] The requirements for accreditation in computing do not include any course or project work that relates to ethical or legal issues in computing, although a more general requirement (that is, one imposed by ABET for accreditation in all relevant disciplines) states that students should graduate with "an understanding of professional, ethical, legal, security and social issues and responsibilities."[99]

Nevertheless, for much of its history as a formal academic discipline, computer science has had a moderately strong norm against providing formal education intended to teach hacking skills.[100] However, in recent years, this norm has started to break down as a number of educational institutions have begun to teach courses explicitly intended to nurture hacking skills.[101] Debate on the topic continues. Teachers of such courses note that they include a substantial ethical treatment in their courses and that their graduates are eagerly sought by government agencies and private sector entities who need people with such skills for carrying out offensive operations against adversary computers or approved "white-hat" penetration testing against an organization's cyber defenses. Detractors dislike the idea of sanctioned or approved cyber intrusions,

97. "ACM Code of Ethics and Professional Conduct," n.d., http://www.acm.org/about/code-of-ethics.

98. "About ABET," n.d., http://www.abet.org/about-abet/.

99. "Criteria for Accrediting Computing Programs, 2016–2017," n.d., http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2016-2017/.

100. See, for example, Eugene H. Spafford, "Are Computer Hacker Break-Ins Ethical?" *Journal of Systems and Software* 41 (17) (1992): 41–47.

101. Ellen Nakashima and Ashkan Soltani, "The Ethics of Hacking 101," *Washington Post*, October 7, 2014, http://www.washingtonpost.com/postlive/the-ethics-of-hacking-101/2014/10/07/39529518-4014-11e4-b0ea-8141703bbf6f_story.html; Jackie Kemp, "The Crack Team," *Guardian*, October 20, 2008, http://www.theguardian.com/education/2008/oct/21/hacking; and Queena Kim, "Good Hack, Bad Hack: A Cybersecurity Camp Teaches the Ethics of Hacking," *Marketplace*, July 2, 2013.

arguing that all vulnerabilities discovered should be promptly reported to parties responsible for fixing them.

Academic researchers do undertake research on vulnerabilities in products and services with the intent of enhancing cybersecurity from the defensive perspective. In doing such work, the expectation of the community is that such research is published, and far from being regarded as antisocial or hostile activity, work to uncover weaknesses is praised by the community because only when such weaknesses become known can they be addressed.

One example is a series of annual workshops on offensive technologies (WOOT) that began in 2007. According to the current description, WOOT aims "to present a broad picture of offense and its contributions, bringing together researchers and practitioners in all areas of computer security. Offensive security has changed from a hobby to an industry. No longer an exercise for isolated enthusiasts, offensive security is today a large-scale operation managed by organized, capitalized actors."[102] But the fundamental rationale for such work is that it informs work on defensive technologies.

Another example is the research community for cryptography. Algorithms for encryption (which scramble and descramble digitally represented data) are designed to be impervious to anything but a "brute-force" attack in which decryption can be reliably accomplished by trying all possible decryption keys. But deep mathematical research can reveal vulnerabilities in an encryption algorithm that allow shortcuts to be taken, thus reducing the effort needed to accomplish a decryption.

Users of encryption algorithms count on such research to reveal weaknesses. As a specific illustration, in 1997 the National Institute of Standards and Technology (NIST) announced the initiation of a development effort for an Advanced Encryption Standard (AES) that would specify one or more encryption algorithms capable of protecting sensitive government information well into the twenty-first century.[103] Some twenty months later, NIST announced a group of fifteen AES candidate algorithms, submitted by members of the cryptographic community from around the world. NIST used an extensive public process to obtain technical commentary on the candidate algorithms, and on the basis of these comments NIST decided on a specific algorithm for the AES.

In general, security researchers also investigate vulnerabilities in deployed products, and many such individuals adhere to an ethic of "responsible disclosure" in which they privately report a discovered vulnerability to the vendor and temporarily withhold public disclosure to give the vendor time to repair it. However, a growing number of such individuals are finding ways to profit from their discoveries, selling them to vendors (which often offer bounties for

102. "9th USENIX Workshop on Offensive Technologies: WOOT '15," Usenix, n.d., https://www.usenix.org/conference/woot15.

103. National Institute of Standards and Technology, "Advanced Encryption Standard (AES) Development Effort," updated February 28, 2001, http://csrc.nist.gov/archive/aes/index2.html.

vulnerabilities) or on the black market to parties for eventual incorporation into cyber weapons.

GOVERNMENT ATTITUDES TOWARD NATIONAL AND INTERNATIONAL GOVERNANCE OF CYBER WEAPONS

All governments are concerned about cyber weapons being used against them and their interests by other nations and nonstate parties—that is, they are concerned about cybersecurity as the term is traditionally defined (i.e., as defense against hostile cyber activities). Furthermore, they are all concerned about the criminal use of cyber weapons—that is, nonstate actors, whether associated with another state or within their own jurisdictional reach, using such weapons for criminal purposes such as fraud, theft, or blackmail.

At the same time, many governments—most often the governments of major world powers—see value in having the ability to use cyber weapons. For example, cyber weapons are useful for espionage operations against other nations, including both government and private sector entities. Cyber weapons also have offensive (and destructive) capabilities that many nations are reluctant to abandon because of their operational advantages. For example, cyber weapons favor the offense in the sense that it is very difficult to erect defenses against them, their use can often be conducted with plausible deniability, the effects of their use can vary broadly, they offer the possibility of asymmetric advantage against nations that are heavily dependent on IT, and they can be relatively inexpensive compared to traditional kinetic weapons. Nonetheless, almost all nations are silent on the question of their national capabilities for conducting offensive operations in cyberspace or even on the possibility that these capabilities might be useful to them. (Apart from the United States, the most significant exception to this general reluctance to discuss matters related to offensive cyber activities is the Dutch Ministry of Defence.)

However, just because governments see value in having access to cyber weapons does not mean they are necessarily sanguine about actually using those weapons. For example, the United States was concerned about the precedent-setting nature of using cyber weapons long before the Stuxnet operation was launched, and even after Stuxnet the United States had similar concerns about the use of such weapons against Libya and in that case chose not to use them.[104] Recent news stories also indicate that Western cyber activities against

104. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009); and Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare against Libya," *New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

the Iranian nuclear infrastructure drove an Iranian cyber retaliation against U.S. financial institutions.[105]

Governments do differ significantly in their willingness to outlaw the use of cyber weapons in a domestic legal context. In some cases, they have a robust legal regime that criminalizes the use of cyber weapons and a willingness to enforce that regime. Most of the signatories of the Budapest Convention are in this category. In other cases, an existing legal regime is accompanied by a reluctance to enforce those laws. Russia is widely regarded as an example.[106]

COMMENTARY AND DISCUSSION

Cyber weapons can play a much different role in conflict than nuclear weapons. The use of a nuclear weapon would be a threshold event of enormous strategic and political significance. By contrast, cyber weapons are being used every day by a broad range of adversaries, ranging from individual misguided teenagers to major nation-states—and many of these uses go entirely unnoticed. Thus, the use of a cyber weapon per se does not cross any kind of threshold. Only if such use resulted in a sufficiently large impact would it do so.

Cyber weapons also have clear value in causing damage if that is the goal. From a policy-maker perspective, nuclear weapons are highly unusable (despite the fact that military planners can easily contemplate their use), and indeed none have been used as a part of hostilities since 1945.[107] Biological weapons have been widely regarded as unpredictable in their effects and of limited value in combat for much of their history, as their use in a conflict might well result in blowback against friendly forces and populations.[108]

105. See David Sanger, "Document Reveals Growth of Cyberwarfare between the U.S. and Iran," *New York Times*, February 22, 2015, http://www.nytimes.com/2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html.

106. See, for example, John Blau, "Russia—A Happy Haven for Hackers," *Computer Weekly*, May 2004, http://www.computerweekly.com/feature/Russia-a-happy-haven-for-hackers.

107. On the other hand, Paul Bracken points out that exploding a nuclear weapon is not the only way to "use" it. Moving nuclear weapons from one place to another or changing the alert status of nuclear delivery vehicles are actions that do not involve exploding nuclear weapons but that still may send politically significant messages. See Paul Bracken, *The Second Nuclear Age* (New York: St. Martin's Griffin Press, 2013).

108. Even real and legitimate concerns about blowback in cyber are not analogous. For biological weapons, blowback is tactical—the same organisms that cause illness in an adversary can cause illness in friendly populations. For cyber weapons, blowback is strategic—launching a cyberattack sets precedents and helps to establish cyberattack as a legitimate means of conflict, but rarely would a cyber weapon be turned back on its user without significant modification. On the use of biological weapons more generally, see Jozef Goldblat, "The Biological Weapons Convention—An Overview," *International Review of the Red Cross*, no. 318 (June 30, 1997), https://www.icrc.org/eng/resources/documents/misc/57jnpa.htm; and Jonathan B. Tucker and Erin R. Mahan, *President Nixon's Decision to Renounce the U.S. Offensive Biological Weapons Program* (Washington, D.C.: National Defense University Press, October 2009), http://wmdcenter.dodlive.mil/files/2011/11/cswmd_cs1.pdf.

In the most general case for any weapon, acquisition requires both physical infrastructure (e.g., laboratories and appropriate physical devices or materials) and appropriate knowledge. For many cyber weapons, the physical infrastructure is not a limiting factor—the computers on which these applications can be developed are ubiquitous. In other cases (especially those in which the intended target is a specific physical system), adequate testing of adversarial applications may require the development and deployment of physical environments that mimic the intended target.[109]

IT and cyber weapons also have a different history than other types of weapons, such as nuclear or biological. The underlying IT is ubiquitous (i.e., more than just broadly available) around the world. Those who create cyber weapons take advantage of this technology base, but they are not—and never have been—primarily researchers. Since (more or less) the first computers, hackers have been curious about how these systems work. What once made the threat from hackers manageable was the small number of computers in the world and the largely prevailing ethos of hackers to refrain from damaging the systems they hacked.

The cyber weapons developed in this early era were derived not from science but from engineering and exploration. Even today, with only a few exceptions, cyber weapons are not created as the result of scientific research on IT and do not involve the discovery of new principles. For example, the penetration aspect of a cyber weapon may involve the discovery of a previously unknown weakness or vulnerability in an existing IT artifact such as a computer program. The payload aspect of a cyber weapon may involve the writing of a new computer program that manipulates the control system of a chemical plant. In neither case would one generally say that new principles were discovered.

Nor are scientific experiments involved in creating cyber weapons. To be sure, cyber weapons may be tested against various targets to understand how they might be made more effective, but such tests generally lack the features that characterize most scientific experiments (e.g., hypothesis testing). In fact, high school students have been developing techniques to penetrate computer systems for many years. (The author of this paper was one such high school student several decades ago.)

Governments fund a considerable amount of scientific research on IT, but since the connection between scientific research and cyber weapons is tenuous at best, research funding is mostly irrelevant to the creation of cyber weapons except insofar as such funding contributes to the overall foundations of IT.

As a result of this history, those interested in the governance of cyber weapons are faced with the problem of creating new institutions and mechanisms where many fewer choke points exist. The inevitable result resembles what is seen today—a paucity of such mechanisms and institutions compared to those

109. For example, the development of Stuxnet required the construction of a test facility containing centrifuges identical to the ones Stuxnet was intended to attack. See Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay."

for biological and nuclear technologies and little prospect for establishing them on a wide scale.

One might imagine that under the rubric of "Internet governance," discussions occur regarding preventing the use of cyber weapons. But in this sphere, there is considerable dispute as to the appropriate participants and what subjects are included under the rubric of "Internet governance," and few if any proposals explicitly address the acquisition or use of cyber weapons.

The dispute in Internet governance regarding participation centers on whether Internet governance is a multi*lateral* endeavor or a multi*stakeholder* endeavor. Those who favor a multilateral approach emphasize the role of national governments as the primary actors in Internet governance. Those who favor a multistakeholder approach identify governments as actors coequal to other stakeholders, such as private sector companies, public interest/civil society groups, and other nongovernment organizations.

The dispute over the purview of Internet governance centers on how, if at all, Internet governance should extend beyond the traditional function of managing IP addresses and domain names. Advocates of extending the scope of "Internet governance" wish to include regulation of various behaviors related to use of the Internet. Certain nations—China and Russia, for example—are strong advocates for the respect of national sovereignty and the right of each nation to define for itself the important aspects of its own history, culture, and social system. From this flows the natural consequence that these governments are concerned not only about cyber weapons that might pass through their borders but also about news stories and other information they find objectionable. (These concerns are generally labeled "information security.") And they insist on the authority to limit their populations' access to such information.

Advocates of restricting the scope of Internet governance to its traditional function reject the proposition that nations should have the right to censor the information to which citizens have access. Concerns about "hostile information" that might be detrimental to state sovereignty conflict directly with the Western tradition of free speech and expression. Thus, a stalemate has existed along these lines for many years.

The debate is complicated by the scope of regulation contemplated by advocates of state-based information control. Specifically, centralized technical measures taken to restrict the use of cyber weapons transmitted through the Internet also conflict with the fundamental underlying design philosophy of the Internet. The Internet was designed in such a way that its only function is to do the best job possible in carrying bits from A to B without regard for the meaning of those bits. Whether those bits are the *New York Times*, a picture of my mother's cats, malicious software embedded in a PDF file, a program for running statistical regressions, or pornography—the Internet is designed to carry it all.

Blocking specific content at the point of receipt—at B—is a relatively straightforward task, assuming that objectionable content can be specified clearly. But in this case, blocking at point B depends on B controlling the deci-

sion to block. Nations that wish to block certain content without B's involvement inevitably resort to more centralized mechanisms located between A and B—that is, in the Internet infrastructure itself. Such changes to the underlying infrastructure would facilitate the fragmentation of the Internet into disparate and perhaps noninteroperable subnetworks.[110]

CONCLUSION

The use of a cyber weapon can have negative effects on data or program integrity (in which data or computer operations are altered with respect to what users expect), on availability (in which services normally provided to users of the system or network are unavailable when expected), and on confidentiality (in which information that users expect to be kept secret is exposed to others).

The agents that might use cyber weapons span a broad range, including lone hackers acting as individuals; criminals acting on their own for profit; organized crime (e.g., drug cartels); transnational terrorists (perhaps acting with state sponsorship or tolerance); small nation-states; and major nation-states. Certain nonstate actors make a business out of using cyber weapons of various kinds against targets of their customers' choosing.

Today, few nations regulate or have laws concerning the creation or acquisition of cyber weapons, notwithstanding export control regimes that seek to prevent "bad" nations from obtaining cyber weapons or related knowledge from the nations that have them and bug bounty programs that reduce the supply of vulnerabilities that may be used to create cyber weapons.

International law is silent on the acquisition or use of cyber weapons, though to the extent that nations agree that the laws of armed conflict apply to cyberspace, some uses of cyber weapons are not permitted. Most nations of the world explicitly endorse the idea of a peaceful cyberspace, though no nation has publicly adopted a policy of refraining from using cyber weapons in its international relations for national security purposes. However, a variety of domestic laws in the nations of the world prohibit the criminal use of cyber weapons in various contexts.

Within the IT community, no broadly accepted and observed norms or codes of behavior proscribe, inhibit, or discourage the technical work needed to uncover vulnerabilities that can be used in cyber weapons. Indeed, those who do such work often receive accolades and financial rewards from IT product and service vendors when those vulnerabilities are revealed so that they may be fixed.

Four primary reasons explain why governance measures regarding cyber weapons have not been widely adopted. First, the underlying technology is ubiquitous, and it is too easy to create cyber weapons. Second, they are too

110. More discussion of this point can be found in David Clark, Tom Berson, and Herbert Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington, D.C.: National Academies Press, 2014).

useful for governments to give up or even to curb. Third, the use of a cyber weapon does not necessarily cross dangerous thresholds—at the lower end, the effect of such use is merely an annoyance or a prank, if that, which means that it is difficult to build cultures to inhibit such behavior per se. At the higher end, the threats posed by the use of cyber weapons are potentially quite serious, even if they are not existential in the same way that the use of nuclear or biological weapons can be. Finally, so many paths lead toward the IT expertise necessary to build cyber weapons that it would be well-nigh impossible for any governance mechanism—or set of governance mechanisms—to intervene effectively to prevent the development of such expertise.

This brief survey of the prospects for governance and oversight for cyber weapons suggests to this author that the future is grim. Cyber weapons have definite utility for national governments (especially in the domain of cyber espionage), and that utility has been demonstrated repeatedly in the last two decades. Accepting negotiated or unilateral constraints on cyber weapons would reduce their utility. Organizations both public and private need to be able to test their systems against cyber weapons that might be used against them (i.e., so-called penetration testing). Add to these points the easy availability of cyber weapons and the lack of meaningful choke points at which governance measures might operate, and one can easily see why few governance measures for cyber weapons exist today.

Concluding Observations

Elisa D. Harris

TECHNOLOGICAL CHARACTERISTICS AND GOVERNANCE PROSPECTS

In a 2006 study the U.S. National Academy of Sciences suggested thinking about the *proliferation* potential of nuclear, biological, and cyber weapons as a continuum or line, with the weapons whose spread was most amenable to nonproliferation efforts—nuclear—on the far left, and the weapons offering the most limited opportunities—cyber—on the far right. Biological weapons fell somewhere between them: not as amenable to nonproliferation efforts as nuclear, but not as limited as cyber.[1] The *governance* potential of these technologies can be thought of as a similar continuum or line, with the technology most amenable to governance efforts—nuclear—again on the far left, and the technology with the most limited opportunities—information technology—on the far right. Biological technology is again somewhere between them.

As the preceding chapters have demonstrated, the position of each of these technologies on a governance continuum is closely related to its characteristics—its history and potential uses; the nature and availability of the relevant material and equipment; the level of effort required to use it for destructive purposes; and its possible effects (see Table 5). Nuclear technology has a special history, having begun as a military technology developed by the government for weapons purposes that later was exploited for civilian applications, primarily energy and research. National governments were and remain central to the development and use of nuclear technology, even in countries where utilities or other private sector entities operate nuclear facilities.

The opposite is true for biological and information technology, which were first and foremost civilian technologies whose destructive potential was recognized only after their legitimate uses had been well established. Biological materials and equipment have extensive civilian uses, including in research, medicine, and agriculture. Information technology also has an unlimited num-

1. Institute of Medicine and National Research Council, *Globalization, Biosecurity, and the Future of the Life Sciences* (Washington, D.C.: National Academies Press, 2006), 53–56, http://www.nap.edu/catalog/11567/globalization-biosecurity-and-the-future-of-the-life-sciences.

ber of legitimate applications. Governments have played an important role in the development and use of both technologies. The first applications of modern information technology, computers, were for military purposes such as code breaking and computations for the atomic bomb. But the most important stakeholders in both the biological and information technology areas are private entities: academic institutions, companies, and individuals.[2]

The nature and availability of the material and equipment, as well as the level of effort needed to use nuclear, biological, and information technology for destructive purposes, also are very different. In the case of a nuclear explosive device, the number of key materials (primarily highly enriched uranium and separated plutonium) and key technologies (enrichment and reprocessing) are limited, although other dual-use materials (such as low enriched uranium and spent fuel) and technologies (nuclear reactors) can also be used. There also are a relatively limited number of countries that possess or can supply the necessary technology. Moreover, although nonstate actors may be able to acquire a so-called dirty bomb, developing a nuclear weapon that will not only work but can be delivered successfully to a target is extremely challenging and costly and requires a dedicated national program.[3]

In contrast to nuclear weapons, a much wider array of materials and equipment can be used to develop biological warfare agents. More than 125 "conventional" pathogens and toxins and nine categories of equipment currently are controlled by Australia Group members because they can be used to produce biological warfare agents. Synthetic biology and other advances in science and technology are expanding the number of potential threat agents still further, as well as the range of practitioners, which includes not only researchers in academic or private laboratories but engineers and others outside the scientific community. Many of the materials and items of equipment used by this broader universe of practitioners are globally available, making the creation of modified or novel pathogens easier and cheaper than ever before. Yet even as the number and type of actors who could develop a dangerous pathogen has proliferated, producing a weapons-grade biological warfare agent and disseminating it effectively remains both technically and operationally much more difficult than generally is believed.

2. Vernon Ruttan, *The Role of the Public Sector in Technology Development: Generalizations from General Purpose Technologies*, Science, Technology, and Innovation Discussion Paper no. 11 (Cambridge, Mass.: Harvard University, Center for International Development, 2001), http://www.cid.harvard.edu/archive/biotech/papers/discussion11_ruttan.pdf.

3. North Korea's nuclear weapons program demonstrates, however, that even a relatively backward and financially strapped country can develop a nuclear capability if it is sufficiently determined and able to secure outside assistance.

Table 5: Characteristics of Nuclear, Biological, and Information Technology

Nuclear Technology	Biological Technology	Information Technology
Military origins	Civilian origins	Civilian origins
Weapons-grade materials difficult, costly to produce	Modified and novel pathogens increasingly easy and cheap to produce; weaponization and dissemination difficult	Many cyber weapons very easy, cheap to produce; higher-end uses challenging
Separated plutonium, highly enriched uranium, low enriched uranium, spent fuel, enrichment and reprocessing equipment, nuclear power reactors	> 125 pathogens and toxins; 9 categories of equipment; threat agents increasing with technological advances	No special materials or facilities; billions of computers with underlying information technology
15 countries with enrichment and/or reprocessing plants; < 10 countries supply enrichment and reprocessing technology and nuclear reactors	Created, stored, and used at wide range of laboratories (government, academic, industry) and private facilities in many countries	Computers and information technology ubiquitous
Limited nonmilitary applications: energy, research	Extensive legitimate applications (e.g., research, medicine, agriculture), including biodefense countermeasures	Unlimited legitimate applications
Can cause massive loss of human life and physical destruction	Can cause massive loss of life (human, animal, and plant) and can contaminate physical infrastructure	Can cause nuisance, large-scale commercial and economic damage; loss of life indirectly

Source: Adapted in part from Jonathan B. Tucker, "Preventing the Misuse of Pathogens: The Need for Global Biosecurity Standards," *Arms Control Today* 33 (5) (June 2003): 3–10.

Rather than special materials or facilities, the key technology used in cyber weapons is information technology. Information technology is available wherever computers are available. Initially, the small number of computers was the determining factor in limiting hostile applications of information technology. Today, an estimated fifteen billion devices around the world are connected to the Internet, a significant portion of which are computers, and the number is growing.[4] Except for high-end uses, cyber weapons also are orders of magnitude easier and cheaper to produce than nuclear explosive devices or biological weapons, as anyone with access to a computer can, in principle, develop such a weapon.

A final characteristic that has influenced the governance potential of each of these technologies is its destructive effects. Since the attacks on Hiroshima

4. Rob Soderbery, "How Many Things Are Currently Connected to the 'Internet of Things' (IoT)?" *Forbes*, January 7, 2013, http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/.

and Nagasaki in 1945, it has been clear that nuclear technology can be used to cause massive loss of life as well as physical damage. While no comparable use of biological technology has occurred, the potential impact, particularly of a highly lethal agent that can spread from person to person, also has been recognized for many years. These concerns about the mass-destruction effects of nuclear and biological weapons have helped stimulate efforts to prevent the spread and use of the relevant technologies, including the negotiation of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Biological Weapons Convention (BWC), and many of the other governance measures discussed in the preceding pages.

In contrast to nuclear and biological weapons, cyber weapons have been used repeatedly and, in some cases, on a large scale for hostile purposes by both national governments and other actors. Some cyberattacks, such as the attack on Estonia's government and media websites and banking services, have resulted in lengthy denials of service throughout the attacked country. Others, like the attack on the Saudi national oil company's computers, disrupted important commercial activities. Still others, such as the Stuxnet attack on Iran's uranium enrichment centrifuges, destroyed vital computer-controlled machinery. A number of other cyberattacks, such as the data breach at the retailer Target, have put tens of millions of customer records at risk. But none of these attacks has led to concerted efforts to control the use of cyber weapons, perhaps in part because no human lives were lost.

These characteristics of nuclear, biological, and information technology go a long way toward explaining the three technologies' differing governance potential. Nuclear technology has been more amenable to governance efforts because its enormous destructive potential has been clear from the outset and because the principal actors involved have been national governments. Even where commercial and other private entities have a stake in nuclear policy, those interests generally are addressed in the internal deliberations within government. Moreover, the dual-use nuclear items that have been the focus of governance, the countries that can supply those items, and the dual-use activities in which they are used are relatively limited, all of which have facilitated governance efforts.

By comparison, everything about cyber weapons runs counter to governance: the underlying technology and the computers on which it is used are deeply embedded in civilian society around the world; the production of most cyber weapons requires no special materials or facilities; and the range of stakeholders—anyone with access to information technology and a computer—is virtually unlimited. Moreover, unlike nuclear and biological weapons, cyber weapons can put human lives at risk only indirectly by, for example, targeting critical infrastructure such as nuclear and chemical facilities, gas pipelines, transit systems, and water supplies.

Biological technology occupies a position between nuclear and information technology on a governance continuum. Biological technology has far

more civilian applications than nuclear technology, but it is not ubiquitous, as is the case with information technology. The range of biological materials and equipment that could produce a highly dangerous pathogen is much larger than with nuclear technology but, even with advances in science, not as widespread as the computers used to launch cyber attacks. The universe of actors that have a stake in biological governance continues to expand well beyond those engaged in nuclear activities but does not include every level of society, as with information technology.

EXISTING DUAL-USE GOVERNANCE MEASURES

Given these differences, it is not surprising that a side-by-side comparison of the types of governance measures that have been adopted in these technology areas reveals the greatest common ground between nuclear and biological technology. As Table 6 shows, various international and national measures have been adopted in an effort to prevent dual-use nuclear and biological technology from being used for weapons purposes. The NPT and the BWC have been central to these efforts, embodying both the norm against destructive applications of these technologies and the specific obligations that give it legal effect. At the national level, many countries have adopted legislation criminalizing the activities prohibited by the treaties and, in the case of the NPT, authorizing International Atomic Energy Agency (IAEA) inspections and monitoring of their civilian nuclear activities.

A much wider range of international and national efforts have sought to control access to dual-use nuclear and biological materials, equipment, and information. Some, such as the export control harmonization activities of the Zangger Committee, the Nuclear Suppliers Group (NSG), and the Australia Group, have focused on denying other countries access to technology that could be used to develop nuclear and biological weapons and thus are important complements to the NPT and BWC. Preventing the spread of weapons and related technology to other countries was also the initial aim of the U.S. Nunn-Lugar Cooperative Threat Reduction program, which helped Russia and other former Soviet republics secure nuclear, biological, and other materials, dismantle former biological weapons facilities, and redirect former weapons scientists to peaceful activities.

Many other measures, particularly since September 11, have sought to deny terrorists access to technology that could be used to develop nuclear and biological weapons. This has been done through a variety of means. For example, under United Nations Security Council Resolution (UNSCR) 1540, all UN member states are obligated to adopt national legislation to prevent terrorists from obtaining materials, equipment, and information for nuclear, biological, and other weapons. Other measures, such as the Proliferation Security Initiative (PSI) and the IAEA Illicit Trafficking Database, are designed to help countries

track and interdict illegal shipments of dual-use materials. Even international industry groups have become involved, with nuclear power plant exporters and two synthetic biology industry associations committing to screen customer orders for the dual-use items they sell. On a national level, antiterrorism legislation in the United States and other countries has tightened domestic controls on biological materials and facilities, as well as on the individuals who have access to them. Similar efforts have been undertaken to ensure the security and safety of domestic nuclear facilities and materials.

Finally, international and national measures have been developed to promote the safe and secure handling and use of dual-use nuclear and biological technology. This includes guidelines on nuclear security issued by the IAEA and guidelines on biosafety and biosecurity issued by the World Health Organization (WHO). It also includes the codes of ethics and conduct promulgated by various international and national scientific organizations to discourage destructive applications of biology. In addition to these nonbinding measures, European Union (EU) member states have enacted controls on the safe handling of genetically modified organisms, based on EU regulations and directives, and Israel and Denmark have enacted legislation requiring prior review and approval of certain categories of dual-use biological research that could raise security concerns.

Table 6: Governance of Nuclear, Biological, and Information Technology

Governance Measure	Nuclear Technology	Biological Technology	Information Technology
International Initiatives Outlawing Hostile/Weapons Activities			
Prohibition on development and possession of dual-use (DU) materials for weapons purposes	Partial (NPT)	Yes (BWC)	No
Prohibition on assisting other countries to acquire DU materials for weapons purposes	Yes (NPT)	Yes (BWC)	No
International oversight of national DU activities and materials to ensure nonuse for weapons purposes	Yes (IAEA safeguards)	No	No
Commitment to adopt national laws outlawing hostile/weapons activities with DU materials	Yes (NPT)	Yes (BWC)	Yes (Budapest Convention)
International Efforts to Control Access to DU Materials			
Requirement to share information on terrorists' efforts to acquire DU materials	Yes (UNSCR 1373)	Yes (UNSCR 1373)	No
Requirement for national measures to prevent terrorists' acquisition/use of DU materials and equipment	Yes (Convention on Physical Protection of Nuclear Materials, amended)	Yes (UNSCR 1540)	No
Commitment to harmonize national controls on transfers of DU materials and equipment to other countries	Yes (Zangger Committee and Nuclear Suppliers Group)	Yes (Australia Group)	Yes (Wassenaar Arrangement)
Commitment to assist countries in eliminating weapons, material, and facilities and redirecting former weapons scientists in former Soviet Union and other countries	Yes (G8 Global Partnership)	Yes (G8 Global Partnership)	No
Commitment to interdict shipments of DU materials to countries/terrorists	Yes (PSI)	Yes (PSI)	No
Assistance to countries in tracking smuggling of DU materials	Yes (IAEA Illicit Trafficking Database)	No	No

Governance Measure	Nuclear Technology	Biological Technology	Information Technology
Assistance to countries in securing DU materials and strengthening laws prohibiting acquisition/use of DU-based weapons	Yes (IAEA Division of Nuclear Security	Yes (INTERPOL Bioterrorism Prevention Program)	No
Commitment by industry to screen orders of DU materials and equipment	Yes (Nuclear Power Plant Exporters)	Yes (International Association Synthetic Biology)	No
International Initiatives on the Handling of DU Materials			
Guidelines for safe handling and use of DU materials	Yes*	Yes (WHO manual)	No
Guidelines for security of DU materials	Yes (IAEA INFCIRC225)	Yes (WHO manual)	No
Codes of ethics/conduct/practice	Yes (World Institute for Nuclear Security)	Yes (InterAcademy Panel)	No
National Initiatives on Hostile/ Weapons Activities			
Prohibition on use of DU materials for hostile/weapons purposes	Yes (IAEA safeguards implementing legislation)	Yes (BWC implementing legislation)	Yes (U.S. Computer Fraud and Abuse Act)
Review of DU R&D activities for compliance with international commitments outlawing hostile/weapons activities	No	Yes (U.S. Department of Defense BWC Compliance Review Group)	No
National Efforts to Control Access to DU Materials			
Controls on transfers of DU materials and equipment to other countries	Yes (export controls by NSG members)	Yes (export controls by EU members)	Yes (export controls by Wassenaar members)
Controls on domestic access to DU materials	Yes (U.S. Nuclear Regulatory Commission [NRC] licensing condition)	Yes (U.S. select agent rules)	No

Governance Measure	Nuclear Technology	Biological Technology	Information Technology
Controls on facilities that possess and use DU materials	Yes (U.S. NRC licensing condition)	Yes (UK Anti-Terrorism Crime and Security Act)	No
Controls on individuals with access to DU materials	Yes (U.S. NRC licensing condition)	Yes (Canadian Human Pathogens and Toxin Act)	No
Commitment to eliminate weapons, material, and facilities and to redirect former weapons scientists in former Soviet Union and other countries	Yes (U.S. Nunn-Lugar)	Yes (U.S. Nunn-Lugar)	No
Guidelines for industry screening of orders for DU materials	No	Yes (U.S. gene sequence screening)	No
National Initiatives on the Handling of DU Materials and Information			
Controls on safe handling/use of DU materials	Yes*	Yes (EU genetically modified organism directives)	No
Requirements for oversight of DU research for security concerns	No	Yes (Danish biosecurity act)	No
Processes for reviewing DU manuscripts for potential security concerns	No	Yes (American Society of Microbiology journals)	No
Codes of ethics/conduct/practice	No	Yes (Dutch Academy of Sciences)	Yes (U.S. ACM code)

Note: The measures listed in parentheses are intended to be illustrative and thus in some cases do not reflect all of the relevant governance measures adopted.

*An extensive body of rules and guidelines concerns nuclear safety, but unlike in the biological area these are entirely distinct from nuclear nonproliferation and nuclear security measures.

In contrast to nuclear and biological weapons, cyber weapons have not been outlawed by international treaty and are in fact being used on a daily basis by a wide range of actors from teenage hackers to national governments. Some of these uses have been highly destructive of commercial and economic interests but thus far have not resulted in the loss of human life. International legal experts have argued that the laws of war and the UN Charter apply to cyberspace and, as such, that some uses of cyber weapons are not permitted. However, even governments like the United States that share this view have been unwilling to forgo the option of using cyber weapons. Moreover, as the experience with the Stuxnet computer worm attack on Iran's nuclear program shows, whether a given use of a cyber weapon is legitimate looks very different depending on whether one is the initiator or the target of the attack.

It is not surprising, therefore, that only a handful of governance measures have been adopted to try to prevent destructive applications of information technology. Internationally, the forty-seven states that are parties to the Budapest Convention on Cybercrime have agreed to enact national legislation criminalizing certain behaviors in cyberspace, such as unauthorized access to a computer or illegal interception of data. Many of these countries, as participants in the Wassenaar Arrangement, also control the export of certain dual-use items that could be used in cyber weapons, such as equipment related to intrusion software or network surveillance systems. At the national level, legislation in various countries also has proscribed certain unauthorized uses of information technology, including to gain access to computers or to intercept electronic communications. In the United States, a society for computer professionals, ACM, also has issued a code of ethics for its members that prohibits them from using computing technology in ways that cause harm.

CHALLENGES TO GOVERNANCE OF DUAL-USE TECHNOLOGY

As the previous chapters have shown, governance efforts in each of the three technology areas have faced serious challenges. Some are a direct result of technical considerations. This is clearly the case in the cyber area, where the absence of choke points, such as specific weapons-related materials or activities, renders efforts to govern the development of cyber weapons nearly impossible. Detecting work on nonnuclear components of nuclear weapons also is technically challenging because such activity does not have an obvious signature, unlike work with nuclear material, which leaves detectable traces.

Other challenges can be linked to scientific and technological advances. This is particularly true in the biological area, where synthetic biology is increasing the number of potential threat agents, the types of equipment used in their development, and the range of practitioners involved, thus greatly complicating efforts to control the transfer of or access to biological agents and technology.

Economic interests also have played an important role in blocking the adoption of governance proposals. This can be seen in the hostility of nuclear reactor exporting countries to tightening the conditions under which reactors or certain reactor components can be transferred to other countries. It also was apparent in the U.S. biotechnology and pharmaceutical industries' opposition to on-site inspections during the failed effort to conclude a compliance protocol to strengthen the BWC.

Still other challenges reflect security interests. The NPT's two-tier system of nuclear "haves" and "have-nots" was necessary because the five nuclear weapons states at the time the treaty was concluded were unwilling to forego the possession of nuclear weapons. Even today, the procurement decisions and operational policies of these countries demonstrate that they continue to see the possession of nuclear weapons as militarily necessary. Security interests also have played a role in the unwillingness of the United States or any other country to formally limit or ban the use of cyber weapons, which can be used in a variety of ways, often without revealing the source of the attack.

Finally, political considerations also have had a significant impact on dual-use governance efforts. Developing countries generally do not share the West's concerns about the risks posed by dual-use biological research and in some cases see governance efforts as little more than a veiled attempt at technology denial. The same is true in the nuclear area, where countries without access to enrichment and reprocessing technology have refused to forego the right to acquire it and even some states that possess such technology have been unwilling to limit their ability to acquire new forms in the future. Efforts to govern cyber weapons also are viewed with little sense of urgency as, unlike nuclear or biological weapons, cyber weapons are not considered weapons of mass destruction whose spread and use must be blocked both internationally and nationally.

GOVERNANCE REQUIREMENTS: KEY LESSONS

These factors help explain the nature of the different governance measures that have been adopted in these three technology areas. They also underscore why a common governance approach is not feasible when it comes to managing the risks from dual-use technologies. This does not mean that the concept of dual-use technology is not useful and should be abandoned. On the contrary, as the previous chapters show, the concept provides a valuable analytical tool for identifying and assessing technologies that have the potential to cause large-scale loss of life or damage to commercial or economic interests even as they continue to be used for legitimate purposes. By analyzing three examples from this category of technologies, as the preceding pages have done, a number of broader lessons become apparent.

One lesson is that governments are unlikely to support restrictions on their use of dual-use technology unless the *stakes* are sufficiently high. To date, the

stakes that have mattered most have been the possible risks to human life. This helps explain the willingness of so many technological "haves" to agree to forego the development of nuclear and biological weapons, as well as the corresponding lack of interest across the international community in restricting the development and use of cyber weapons.

A second lesson is that in the absence of genuine and broad agreement on the threat, governments are unlikely to support restrictions on their acquisition and use of dual-use technology unless the *rewards* for doing so are sufficiently high. This is demonstrated by the insistence of the technological "have-nots" on access to nuclear and biological technology as a quid pro quo for foregoing the acquisition of nuclear and biological weapons. It is also demonstrated by the experience of cyber weapons, whose underlying information technology already is widely available around the globe, thus limiting not only the security benefits but also any technology benefits that might accrue from supporting restrictions on technology used for cyber weapons.

Finally, unless governments and other relevant stakeholders view governance of dual-use technology as a *collective responsibility*, efforts to manage the relevant risks are likely to be limited at best. This is demonstrated by the lack of enthusiasm for bold proposals to strengthen the nuclear nonproliferation regime, such as former IAEA Director Mohamed ElBaradei's suggestion to internationalize the nuclear fuel cycle. It is also demonstrated by the preference of scientists and scientific organizations for self-governance rather than independent oversight and for codes of conduct and other voluntary measures rather than legal requirements to address concerns about certain types of dual-use biological research. And it is demonstrated by the reluctance of national governments and the information technology industry to countenance measures other than export controls and codes of conduct to address the problem of cyber weapons.

RECENT AND FUTURE STEPS

Notwithstanding the pessimism reflected above, as this volume is being completed, there are indications of additional progress in managing the risks from the three dual-use technologies that are its focus. In the case of nuclear technology, the July 2015 agreement limiting Iran's nuclear program in exchange for the lifting of economic sanctions has been approved by the Iranian Parliament and is now being implemented. This agreement, which was concluded by Iran, the P5+1 (the United States, United Kingdom, France, China, Russia, and Germany), and the European Union, includes unprecedented elements, including the application of advanced safeguards technology, transparency into Iran's uranium supply chain, time-limited dispute resolution procedures for access to

suspect sites, and snap-back sanctions procedures.[5] These elements go beyond the terms of existing nuclear nonproliferation measures and, as such, may serve as a model not only for resolving concerns about other nuclear weapons programs but also for strengthening the broader international nuclear nonproliferation regime.

In the cyber area, progress has been made toward creating what President Barack Obama calls "an architecture to govern behavior in cyberspace that is enforceable and clear."[6] This is seen in the September 2015 agreement by Presidents Xi Jinping and Obama not to conduct or knowingly support cyber-enabled theft of intellectual property. The two leaders also welcomed the July 2015 UN Group of Governmental Experts on Information, Telecommunications, and International Security (GGE) report on cybersecurity that, among other things, recommended that states not conduct or knowingly support cyber activity that intentionally damages or impairs the ability of critical infrastructure to provide services to the public.

Differences remain on whether the two nations' cybersecurity commitment applies to cybercrime or the broader problem of cyber espionage and, potentially, on what is meant by *critical infrastructure*, which was not defined in the 2015 GGE report. Moreover, the United States has made clear that it could still impose sanctions on Chinese entities if they continue hacking U.S. companies, as appeared to be the case in the aftermath of the U.S.-China announcement.[7] Nevertheless, China's apparent willingness to forgo computer theft of intellectual property and cyberattacks on critical infrastructure represents an important step. The same is true of the subsequent statement by the G20, in November 2015, opposing cyber theft of intellectual property and affirming the role of the UN Charter in governing state behavior in the use of information and communications technologies.

In the case of biological technology, the U.S. government has taken modest steps to strengthen safety and security at facilities that work with select agents. Like the deliberative process for gain of function (GOF) research, these steps were a direct result of the incidents revealed in 2014 involving the mishandling of dangerous pathogens at federal facilities. In late 2015, the White House announced that it was moving forward with the recommendations in the December 2014 Federal Experts Security Advisory Panel (FESAP) report, including those involving select agent deactivation procedures, laboratory incident reporting, and high-containment laboratory requirements. Determining the latter is especially important given the proliferation of U.S. high-contain-

5. For details on the Iran agreement, see White House, "The Historic Deal That Will Prevent Iran from Acquiring a Nuclear Weapon," n.d., https://www.whitehouse.gov/issues/foreign-policy/iran-deal.

6. David E. Sanger, "Path Set by U.S. and China to Limit Security Breaches May Be Impossible to Follow," *New York Times*, September 26, 2015.

7. Julie Hirschfield Davis and David E. Sanger, "U.S. and China Agree to Rein in State-Sponsored Computer Thefts," *New York Times*, September 26, 2015; and Paul Mozur, "Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies," *New York Times*, October 19, 2015.

ment laboratories working with dangerous pathogens over the past decade. The White House also outlined its plans for implementing the recommendations of another review panel, the Fast Track Action Committee on Select Agent Regulations (FTAC-SAR), which had issued a report in October 2015. One of the committee's most important recommendations is for international engagement to explore opportunities for harmonizing biosecurity standards, but it is not clear whether the administration agrees with this objective.

There is still much that the U.S. government should do to reduce the risks from biotechnology research. GOF studies of concern should be added to the select agent regulations. This can be done by the executive branch and does not require legislative action. A more robust approach to oversight of other types of dual-use research of concern should also be adopted. The experience of the past decade underscores what such an oversight process should entail. It should be mandatory and apply without exception to all relevant research, irrespective of whether the work is done in government or nongovernment institutions, or whether it is unclassified or classified. It should clearly define the categories of research that are subject to the oversight requirements, which should be coordinated and overseen by an independent federal entity. And as yet another expert committee has now recommended, it should seek to harmonize U.S. biosecurity requirements internationally.

All of this underscores a broader theme: rather than a single or best solution, measures aimed at governing dual-use technologies have been and will continue to evolve incrementally, focus on different aspects of the problem, and take various forms, as no individual measure on its own can effectively address the full range of potentially adverse consequences. This is clear in the multiplicity of measures that have been adopted over the past half century to manage the risks from nuclear and biological technology. Taken together, these measures have helped to prevent the development and use of these technologies for hostile purposes. They also have helped to control access to and promote the safe and secure handling of the materials, equipment, and information associated with them.

More can still be done—and needs to be done—by governments and other stakeholders to help prevent the use of nuclear, biological, and information technology from causing large-scale human, economic, or commercial harm. This study delineates some of the technical, scientific, economic, security, and political challenges facing those efforts. It also has identified some of the broader lessons from the governance experience with these technologies, including the potential for further measures, albeit incremental in nature, to help ensure that their social benefits can and will continue to be realized.

List of Acronyms

ABET	Accreditation Board for Engineering and Technology
ACM	Association for Computer Machinery
AES	Advanced Encryption Standard
AG	Australia Group
ASM	American Society of Microbiology
ATCSA	Anti-Terrorism, Crime and Security Act
BMBL	*Biosafety in Microbiological and Biomedical Laboratories*
BRC	biological resource centers
BWC	Biological Weapons Convention
CAD	computer-aided design
CAM	computer-aided manufacturing
CBB	Center for Biosecurity and Biopreparedness
CBMs	confidence-building measures
CCL	Commerce Control List
CDC	Centers for Disease Control and Prevention
CETR	Centers of Excellence for Translational Research
CFAA	Computer Fraud and Abuse Act
COBRAT	Steering Committing on Biotechnological Research in an Age of Terrorism
CPPNM	Convention on the Physical Protection of Nuclear Material
CRG	Compliance Review Group
CTR	Nunn-Lugar Cooperative Threat Reduction
DDOS	distributed denial of service
DHS	Department of Homeland Security
DOD	Department of Defense
DU	dual-use
DURC	dual-use research of concern
EAA	Export Administration Act
EC	European Commission; European Council
ECPA	Electronic Communications Privacy Act
EPA	U.S. Environmental Protection Agency
EU	European Union
FBI	Federal Bureau of Investigations
FESAP	Federal Experts Security Advisory Panel
FTAC-SAR	Fast Track Action Committee on Select Agent Regulations
FY	fiscal year
GOF	gain of function
GGE	Group of Governmental Experts on Information, Telecommunications, and International Security

GMOs	genetically modified organisms
HEU	highly enriched uranium
HHS	Department of Health and Human Services
HPAI	highly pathogenic avian influenza
IAEA	International Atomic Energy Agency
IAP	InterAcademy Panel
IBC	institutional biosafety committees
ICSANT	International Convention for the Suppression of Acts of Nuclear Terrorism
ICT	information and communications technology
IRB	institutional review boards
IRE	institutional review entity
IT	information technology
ITAR	International Traffic in Arms Regulations
KNAW	Royal Netherlands Academy of Arts and Sciences
LEU	low enriched uranium
LOAC	law of armed conflict
MERS	Middle East respiratory syndrome
NAS	National Academy of Sciences
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
NRC	Nuclear Regulatory Commission
NSABB	National Science Advisory Board for Biosecurity
OECD	Organisation for Economic Co-Operation and Development
PI	primary investigator
PSI	Proliferation Security Imitative
R&D	research and development
RAC	Recombinant DNA Advisory Committee
RCEs	Regional Centers of Excellence
RDT&E	research, development, test, and evaluation
SARS	severe acute respiratory syndrome
SERCEB	Southeast Regional Center of Excellence for Emerging Infections and Biodefense
UN	United Nations
UNSCR	UN Security Council Resolution
USCYBERCOM	United States Cyber Command
USDA	U.S. Department of Agriculture
USML	United States Munitions List
WHO	World Health Organization
WMD	weapons of mass destruction
WOOT	workshops on offensive technologies

Contributors

James M. Acton is Co-Director of the Nuclear Policy Program and a Senior Associate at the Carnegie Endowment for International Peace. His work spans the field of nuclear policy. Acton recently published *Wagging the Plutonium Dog: Japanese Domestic Politics and its International Security Implications*, and is the author of two Adelphi books, *Deterrence During Disarmament: Deep Nuclear Reductions and International Security* and *Abolishing Nuclear Weapons* (with George Perkovich). He wrote, with Mark Hibbs, the highly cited study *Why Fukushima Was Preventable*. An expert on hypersonic conventional weapons and the author of *Silver Bullet?: Asking the Right Questions about Conventional Prompt Global Strike*, Acton has testified on this subject to the U.S. House of Representatives Armed Services Committee and the congressionally chartered U.S.-China Economic and Security Review Commission. He is a member of the Commission on Challenges to Deep Cuts and of the Nuclear Security Working Group. Acton has published in *The New York Times*, the *International Herald Tribune*, *Foreign Affairs*, *Foreign Policy*, *Survival*, *The Washington Quarterly*, and *Science and Global Security*. He holds a PhD in theoretical physics from the University of Cambridge.

Elisa D. Harris is a non-resident Senior Research Scholar at the Center for International and Security Studies at Maryland (CISSM). From 1993 to 2001, she was Director for Nonproliferation and Export Controls on the National Security Council staff, where she had primary responsibility for coordinating U.S. policy on chemical, biological, and missile proliferation issues. Ms. Harris has held a number of research positions, including in the Foreign Policy Studies program at the Brookings Institution, the Royal United Services Institute for Defence Studies in London, and the Center for Science and International Affairs at Harvard University. She is a former SSRC-MacArthur Foundation Fellow in International Peace and Security Studies and staff consultant to the Committee on Foreign Affairs, U.S. House of Representatives. Ms. Harris is the author of numerous publications on chemical and biological weapons issues and has testified frequently before the U.S. Congress. She has an A.B. in Government from Georgetown University and an M.Phil in International Relations from Oxford University.

Herbert Lin is Senior Research Scholar for cyber policy and security at the Center for International Security and Cooperation and Research Fellow at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in and knowledgeable about the use of offensive operations in cyberspace, especially as instruments of national policy. In addition to his positions at Stanford University, he is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986–1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Robert Rosner is a theoretical physicist, on the faculty of the University of Chicago since 1987, where he is the William E. Wrather Distinguished Service Professor in the departments of Astronomy & Astrophysics and Physics, as well as in the Enrico Fermi Institute, the Computation Institute, and the Harris School of Public Policy Studies. He served as Argonne National Laboratory's Chief Scientist and Associate Laboratory Director for Physical, Biological and Computational Sciences (2002–2005), and was Argonne's Laboratory Director from 2005–2009; he was the founding chair of the U.S. Department of Energy's National Laboratory Directors' Council (2007–2009). He was elected to the Norwegian Academy of Science and Letters (as a Foreign Member) in 2004; he is also a Fellow of the American Physical Society. Most of his scientific work has been related to fluid dynamics and plasma physics problems, as well as in applied mathematics and computational physics, especially in the development of modern high-performance computer simulation tools, with a particular interest in complex systems (ranging from astrophysical systems to nuclear fission reactors). Within the past few years, he has been increasingly involved in energy technologies, and in the public policy issues that relate to the development and deployment of various energy production and consumption technologies, including especially nuclear energy, the electrification of transport, and energy use in urban environments. As an outgrowth of these interests, he co-founded the Energy Policy Institute (EPIC) at the University of Chicago, spanning the Harris School of Public Policy Studies, the Booth School of Business, and the Department of Economics. He was elected to the American Academy of Arts and Sciences in 2001. He is a member of the Academy's Council and serves as Cochair of the Academy's Global Nuclear Future Initiative.

American Academy of Arts & Sciences
Cherishing Knowledge, Shaping the Future

Since its founding in 1780, the American Academy has served the nation as a champion of scholarship, civil dialogue, and useful knowledge.

As one of the nation's oldest learned societies and independent policy research centers, the Academy convenes leaders from the academic, business, and government sectors to address critical challenges facing our global society.

Through studies, publications, and programs on Science, Engineering, and Technology; Global Security and International Affairs; the Humanities, Arts, and Education; and American Institutions and the Public Good, the Academy provides authoritative and nonpartisan policy advice to decision-makers in government, academia, and the private sector.

American Academy of Arts & Sciences

Selected Publications of the American Academy

The Back-End of the Nuclear Fuel Cycle: Establishing a Viable Roadmap for a Multilateral Interim Storage Facility by Robert Rosner, Lenka Kollar, and James P. Malone

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes by Matthew Bunn and Scott D. Sagan

Nuclear Power in Vietnam: International Responses and Future Prospects by Tanya Ogilvie-White

Nuclear Liability: A Key Component of the Public Policy Decision to Deploy Nuclear Energy in Southeast Asia by Mohit Abraham

The Back-End of the Nuclear Fuel Cycle: An Innovative Storage Concept by Stephen M. Goldberg, Robert Rosner, and James P. Malone

Lessons Learned from "Lessons Learned": The Evolution of Nuclear Power Safety after Accidents and Near-Accidents by Edward D. Blandford and Michael M. May

Multinational Approaches to the Nuclear Fuel Cycle by Charles McCombie and Thomas Isaacs, Noramly Bin Muslim, Tariq Rauf, Atsuyuki Suzuki, Frank von Hippel, and Ellen Tauscher

Nuclear Collisions: Discord, Reform & the Nuclear Nonproliferation Regime by Steven E. Miller, Wael Al-Assad, Jayantha Dhanapala, C. Raja Mohan, and Ta Minh Tuan

Game Changers for Nuclear Energy by Kate Marvel and Michael May

Nuclear Reactors: Generation to Generation by Stephen M. Goldberg and Robert Rosner

Shared Responsibilities for Nuclear Disarmament: A Global Debate by Scott D. Sagan, James M. Acton, Jayantha Dhanapala, Mustafa Kibaroglu, Harald Müller, Yukio Satoh, Mohamed I. Shaker, and Achilles Zaluar

"On the Global Nuclear Future," vols. 1–2, *Daedalus*, 2009–2010

To order any of these publications please contact the Academy's Publications Office. Telephone: 617-576-5085; Fax: 617-576-5088; Email: publications@amacad.org

AMERICAN ACADEMY OF ARTS & SCIENCES