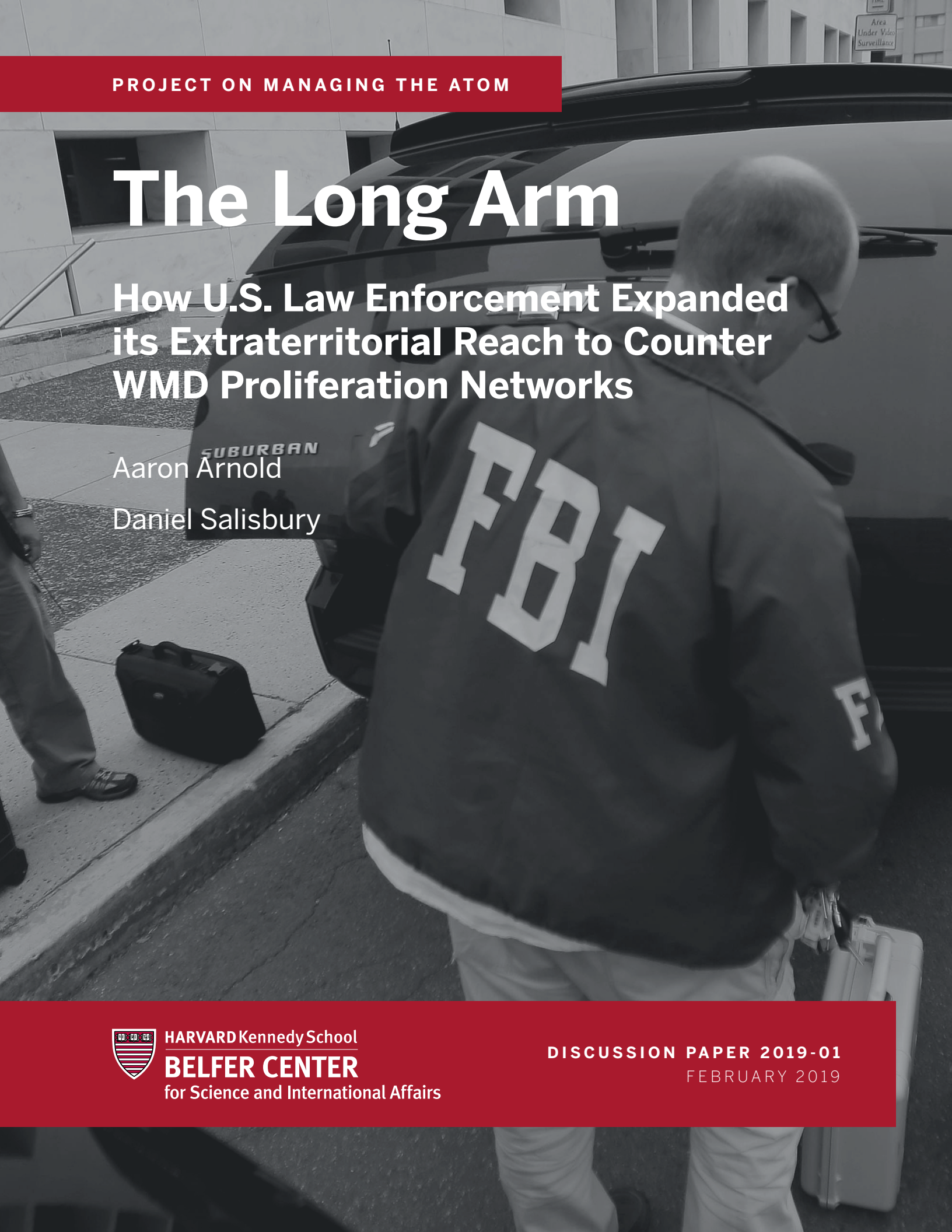

PROJECT ON MANAGING THE ATOM

The Long Arm

How U.S. Law Enforcement Expanded its Extraterritorial Reach to Counter WMD Proliferation Networks

Aaron Arnold

Daniel Salisbury

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DISCUSSION PAPER 2019-01
FEBRUARY 2019

Project on Managing the Atom
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/MTA

Aaron Arnold and Daniel Salisbury, "The Long Arm: How U.S. Law Enforcement Expanded its Extraterritorial Reach to Counter WMD Proliferation Networks," (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, February 2019).

Design and Layout by Jacob Carozza

Cover photo: FBI agents leave a raid in Trenton, N.J. on July 19, 2012 (Julio Cortez/Associated Press).

Printed in the United States of America

PROJECT ON MANAGING THE ATOM

The Long Arm

How U.S. Law Enforcement Expanded its Extraterritorial Reach to Counter WMD Proliferation Networks

Aaron Arnold

Daniel Salisbury

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DISCUSSION PAPER 2019-01
FEBRUARY 2019

Acknowledgments

The authors would like to sincerely thank Martin Malin, Matt Bunn, Will Tobey, Rolf Mowatt-Larssen, Steven E. Miller, Robert Shaw, and Kenneth MacDonald, as well as those law enforcement and intelligence professionals who wish to remain nameless, for their helpful comments. The authors would also like to thank Jacob Carozza and Humza Jilani, who assisted with the editing and preparation of the report, as well as Amber Morgan and Alex O'Neill for assistance with background research efforts. Research for this report was supported by grants from the Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation.

About the Project on Managing the Atom

The Project on Managing the Atom (MTA) is the Harvard Kennedy School's principal research group on nuclear policy issues. Established in 1996, the purpose of the MTA project is to provide leadership in advancing policy-relevant ideas and analysis for reducing the risks of nuclear and radiological terrorism; stopping nuclear proliferation and reducing nuclear arsenals; lowering the barriers to safe, secure, and peaceful nuclear energy use; and addressing the connections among these problems. Through its fellows program, the MTA project also helps to prepare the next generation of leaders for work on nuclear policy problems. The MTA project provides its research, analysis, and commentary to policy makers, scholars, journalists, and the public.

E-mail: atom@hks.harvard.edu
Website: http://belfercenter.org/MTA

About the Authors

Aaron Arnold is a Research Fellow with the Project on Managing Atom at the Belfer Center for Science and International Affairs. His current work focuses on the implementation and enforcement of trade controls for preventing WMD proliferation. Prior to his current position, he worked as a nonproliferation and counterproliferation subject matter expert at the U.S. Department of Defense and U.S. Justice Department, where he specialized in threat finance and sanctions evasion. Aaron holds a PhD and MPP in public policy and national security from George Mason University and a BA in international relations from Virginia Tech.

Daniel Salisbury is a Research Fellow at the Centre for Science and Security Studies (CSSS), Department of War Studies at King's College London. He is also an Associate and a former Stanton Nuclear Security Fellow with the Project on Managing the Atom. Daniel holds a PhD, MA in Science and Security and a BA in War Studies from King's College London.

Table of Contents

Executive Summary 1

Findings and Recommendations 2

Report Organization 4

Section 1: Cutting off the Supply of WMD Technology 6

U.S. Coordination and Capacity Building Efforts 9

Domestic U.S. Authorities for Counterproliferation Law Enforcement 14

Domestic U.S. Implementation and Enforcement 18

Summary 21

Section 2: Overseas Counterproliferation Investigations and Operations 23

Counterproliferation and the Challenge of Jurisdiction 26

U.S. Legal Dimensions of Extraterritoriality 30

U.S. Extraterritorial Counterproliferation Operations 33

The Intersection of Law Enforcement and Regulation 42

Implications of Expanding Law Enforcement Counterproliferation Extraterritoriality 51

Section 3: Recommendations and Conclusions 55

Enhancing Domestic Integration and Collaboration 55

Maintaining both Capability and Legitimacy 57

Increasing Financial Transparency 60

Conclusion 62

FBI agents leave a raid in Trenton, N.J. on July 19, 2012.
Julio Cortez/Associated Press

Executive Summary

The networks of middlemen and intermediaries involved in the illicit procurement of weapons of mass destruction (WMD)-related goods and technologies often operate outside of the United States, which presents several legal and political challenges regarding U.S. trade control enforcement activities. This report considers the extraterritorial efforts of U.S. law enforcement in counterproliferation-related activities and their implications. In other words, how does the United States contend with violations of its weapons of mass destruction (WMD)-related trade controls in overseas jurisdictions, and what are the implications for broader U.S. and international nonproliferation efforts, as well as wider international security and economic concerns?

In recent decades, North Korea and Iran have demonstrated a keen ability to exploit lax governance and oversight in various countries to illicitly procure WMD-related and dual-use goods and technologies—i.e., goods and technologies that have both WMD and civilian applications—in the international marketplace. Even countries with sophisticated indigenous capabilities, like China, India, and Pakistan, continue to illicitly procure these goods and technologies through black and grey markets. Illicit suppliers and middlemen, for example, have frequently used circuitous routes, acquiring goods through third countries and transshipping them in order to avoid the scrutiny of law enforcement, intelligence, and regulatory agencies. In order to address these gaps, the United States, in concert with international partners, has taken significant steps to ensure states make concrete commitments to implement supply-side controls in order to prevent the spread of WMD-related goods and technologies. The United States has promoted stronger controls on illicit trade through law enforcement and intelligence cooperation, industry outreach, and capacity-building and training efforts. In principle, while other countries face similar challenges with extraterritorial enforcement, the United States has been the most aggressive.

Despite international commitments to implementing national trade controls, significant gaps in financial, supply-chain, and logistical systems remain, mainly due to political and legal differences between foreign ju-

risdictions. In response, U.S. law enforcement has adopted a wide range of counterproliferation activities to contend with jurisdictional hurdles. Take, for example, the case of Karl Lee—a "principal contributor" to Iran's ballistic missile program. Karl Lee (aka Li Fang Wei) is a China-based businessman who, since the early 2000s, according to U.S. prosecutors, supplied Iran's ballistic missile program with advanced technologies and controlled materials, such as graphite, specialty metal alloys, gyroscopes, accelerometers, and various machine tools and manufacturing equipment. Some of the goods, like graphite, appear to have been produced in his factory located in Dalian, China. In 2014, open source records suggested that Lee expanded his manufacturing operations beyond graphite, to include fiber optic gyroscopes—a critical component used in missile guidance systems.[1] The Karl Lee case helps to illustrate a particularly tough problem when it comes to WMD proliferation: jurisdiction. That is, what can the United States do to counter networks and middlemen that traffic in WMD-related goods and technologies who are located in foreign jurisdictions where authorities are unwilling to work with U.S. officials or their allies?

Findings and Recommendations

This report finds that while conducting extraterritorial enforcement demonstrates a strong commitment to controlling the spread of WMD-related goods and technology and that U.S. tools and efforts in this area are expanding, such actions can also erode trust and may undermine efforts to ensure consistent implementation of trade control norms and obligations, such as those found in UN Security Council Resolution 1540.

Overall, this report recommends that the United States should work toward finding a balance between extraterritorial law enforcement activities and ensuring a consistent and multilateral approach to global nonproliferation objectives—especially for implementing global strategic trade con-

1 Daniel Salisbury and Ian Stewart, "Li Fang Wei (Karl Lee) Proliferation Case Study Series" (London: Project Alpha, Centre for Science and Security Studies, King's College London, May 19, 2014). As of 2018, evidence indicates that Lee is still active. In addition to new websites, company names, and contact information, Lee most recently listed job advertisements for "foreign trade export specialists," as well as individuals with expertise in using computer numerical control (CNC) and carbon fiber winding machines. Daniel Liu, "Karl Lee, Where Is He Now?" (London: Project Alpha, Centre for Science and Security Studies, King's College London, October 26, 2018).

trols. In order to enhance U.S. counterproliferation efforts in this area, we make three general recommendations:

- **Recommendation 1.** Currently, counterproliferation-related law enforcement activities are spread across several agencies of the U.S. government with few points of integration. The inter-agency mechanisms that do exist for coordination—like the Export Enforcement Coordination Center—are limited in terms of scope, participation, and funding. Moreover, the United States lacks a national counterproliferation law enforcement strategy. Consequently, enforcement—at times—can appear *ad hoc* and produce counterproductive results concerning broader nonproliferation goals and objectives. In order to more effectively coordinate extraterritorial enforcement activities, the Trump administration should appoint a director for counterproliferation law enforcement on the National Security Council staff, under the Senior Director for nonproliferation, responsible for developing a national strategy that integrates broader U.S. and international counterproliferation objectives. The director should also conduct a comprehensive assessment of U.S. counterproliferation law enforcement activities, focusing on ways to reduce redundancy and overlap by increasing information-sharing and coordination. Such an assessment should also explore ways to maximize the efficacy of inter-agency cooperation.

- **Recommendation 2.** The United States must calibrate its extraterritorial enforcement efforts in order to prevent overuse and ensure future capability. As a consequence of U.S. unilateral sanctions policies, countries and non-state actors are adapting to minimize and mitigate exposure to U.S. legal and regulatory risks. Extraterritorial law enforcement actions may contribute to this trend and ultimately undermine broader U.S. and international nonproliferation objectives and commitments, as well as broader international security and economic concerns. Instead, preference should be given to options that make use of official legal procedures while adhering to international rules and norms, in the service of nonproliferation objectives that enjoy international support—like

adherence to and implementation of Resolution 1540. Multilateral cooperation should remain a cornerstone of U.S. counterproliferation efforts. The Department of State, in concert with the Departments of Treasury and Justice, should work to update bilateral legal assistance treaties to incorporate legal definitions and standards consistent with contemporary interpretations of jurisdiction for export controls and nonproliferation objectives.

- **Recommendation 3.** Finally, the United States should continue to focus on deterring, preventing, and disrupting illicit procurement networks by taking broader steps to constrain proliferators' use of "enabling institutions," such as secrecy jurisdictions within the United States and overseas. It is essential that U.S. counterproliferation law enforcement continue to examine and question its assumptions and conventional wisdom about the nature of illicit procurement. A practical law enforcement approach needs to be based on a sound understanding of the causes and consequences of illicit procurement, to include: motivations, *modus operandi*, and processes of adaptation.

Report Organization

Using open source information, interviews with current and former law enforcement officials, and reviews of court records and proceedings, this report provides a detailed assessment of current U.S. law enforcement efforts for countering WMD proliferation, the legal and political challenges the United States faces, and the implications of U.S. enforcement efforts for broader nonproliferation, foreign policy, and economic goals. In Section 1 we review the U.S. and international commitments to implement supply-side controls to prevent the spread of WMD-related goods and technologies and highlight current gaps and challenges. Section 2 considers U.S. law enforcement efforts to counter proliferation activities that occur in foreign jurisdictions. These include undercover and sting operations, the use of lure techniques, information operations, as well as new tools at the nexus between law enforcement and regulation. Section 2 concludes with a discussion of how these tools may impact broader nonproliferation efforts.

Finally, section 3 offers recommendations to enhance law enforcement for counterproliferation while avoiding potential unintended consequences of increased extraterritorial enforcement.

Section 1: Cutting off the Supply of WMD Technology

History has repeatedly shown that states seeking WMD have relied—at least partially—on acquiring foreign materials and technologies.[2] During the 1980s and 1990s, for example, Pakistan and Iraq covertly sourced sensitive nuclear enrichment components from international suppliers.[3] According to recent United Nations (UN) reports, North Korea continues to supply its nuclear and ballistic missile programs from foreign manufacturers, despite strict international sanctions regimes and trade controls.[4] Although Iran agreed to curb its nuclear program following the 2015 Joint Comprehensive Plan of Action (JCPOA), the country continues to illicitly procure foreign materials for use in its ballistic missiles.[5]

Given states' apparent and persistent need to source WMD-related goods and technologies from foreign suppliers, beyond a keen interest in curbing the demand for WMD, policymakers have focused a great deal of attention on supply-side controls (e.g., multilateral and national export-controls, targeted financial sanctions regimes, and embargoes, among other legal and regulatory actions). At the very least, restricting the supply of critical equipment, technology, and materials may be a useful stop-gap to curbing demand—albeit, one more likely to slow rather than prevent the eventual success of a WMD program.[6] Although this report does not directly address the efficacy of multilateral supply-side regimes, it is essential to

2 Scott Sagan, "Why Do States Build Nuclear Weapons? Three Models in Search of a Bomb," *International Security*, Vol. 21 (January 1, 1997), pp. 54–86; Chaim Braun and Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime," *International Security*, Vol. 29, No. 2 (October 1, 2004), pp. 5–49; Vipin Narang, "Strategies of Nuclear Proliferation: How States Pursue the Bomb," *International Security*, Vol. 41, No. 3 (2016), pp. 110–150; Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network," *International Security*, Vol. 30, No. 2 (October 1, 2005), pp. 153–187.

3 Feroz Khan, *Eating Grass: The Making of the Pakistani Bomb* (Palo Alto: Stanford University Press, 2012); David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010).

4 "Report of the Panel of Experts Established Pursuant to Resolution 1874" (United Nations Security Council, March 5, 2018).

5 U.S. Department of the Treasury, Press Release, "Treasury Sanctions Supporters of Iran's Ballistic Missile Program and Iran's Islamic Revolutionary Guard Corps—Qods Force," (Washington, D.C., February 3, 2016,) https://www.treasury.gov/press-center/press-releases/Pages/as0004.aspx (accessed February 11, 2019).

6 Matthew Kroenig, "Exporting the Bomb: Why States Provide Sensitive Nuclear Assistance," *The American Political Science Review*, Vol. 103, No. 1 (February 2009), pp. 113–133; Matthew Fuhrmann, "Exporting Mass Destruction? The Determinants of Dual-Use Trade," *Journal of Peace Research*, Vol. 45, No. 5 (September 1, 2008), pp. 633–652.

understand the general scope and parameters of the regimes. Equally, export controls are one facet of a layered and multidimensional regime that requires cooperation and coordination among diplomatic, intelligence, regulatory, law enforcement, and commercial resources.[7] Within this landscape, enforcement represents a narrow range of activities—extraterritorial enforcement is even more narrow. However, given the significant power and reach of U.S. enforcement efforts, it is important to fully understand how the United States has approached enforcement, its evolution, and its potential unintended consequences for other intelligence, law enforcement, and diplomatic efforts.

Early on in the post-WWII years, the United States and its allies recognized the importance of controlling exports of strategic goods and technologies. Established in 1949, the Coordinating Committee for Multilateral Export Controls (CoCom) was one of the first informal arrangements between Western powers to deny strategic technologies to the then-Soviet Union. To be sure, many viewed the CoCom as nothing more than a "gentleman's handshake" with little or no authority to address violations—most of which were dealt with in secret.[8] Although the CoCom ceased its operations by 1994, several multilateral and international arrangements, including the Nuclear Suppliers Group (NSG), the Wassenaar Arrangement, the Missile Technology Control Regime (MTCR), and the Australia Group, have emerged and endured as supplier states have increasingly harmonized their export controls.[9]

As global trade and commerce boomed throughout the 1990s, controlling proliferation-sensitive goods and technologies required increasing levels of cooperation and coordination among diverse political, legal, and regulatory systems. Different concepts of ownership and jurisdiction (i.e., what a country considers as part of its legal territory), as well as different political

7 Bunn et al., for example, explain the need for consistent and integrated approaches to preventing illicit trade in WMD proliferation-related goods and technologies. See, Matthew Bunn, Martin B. Malin, William C. Potter, and Leonard S. Spector, *Preventing Black Market Trade in Nuclear Technology* (New York: Cambridge University Press, 2018), pp. 323–363.

8 John H. Gibbons, *Technology and East-West Trade*, ed. Technology and East-West Trade Advisory Panel (Washington, D.C.: Congress of the United States, Office of Technology Assessment, 1981), p. 160.

9 The NSG controls nuclear technologies; Wassenaar is aimed at military technologies; MTCR focuses on missile technology; Australia Group controls trade in chemical and biological technologies. As of August 2018, only 30 states belong to all four export-control regimes.

and policy objectives, have frustrated states' efforts to form an international consensus on what *should* and *should not* be controlled, and more broadly constrained the implementation of supply-side measures.[10] For example, it was not until 1992 that the Nuclear Suppliers Group included dual-use goods and technologies in its guidelines (i.e., goods and technologies that could make a "major contribution to an unsafeguarded nuclear fuel cycle or nuclear explosive," but also have non-nuclear uses).[11]

As A.Q. Khan's nuclear proliferation network unraveled in the early 2000s, it was clear that global export control regimes—at the time—were unprepared to deal with non-state WMD proliferation. His network employed layers of middlemen, suppliers, and financiers from Europe and South East Asia to the Middle East in order to acquire, manufacture, and sell nuclear enrichment technologies, weapons plans, and other dual-use goods to Iran, Libya, and North Korea.[12] The Nuclear Suppliers Group, the Australia Group, the Missile Technology Control Regime, and the Wassenaar Arrangement were each informal, multilateral agreements between states that provided guidelines and established norms for implementing domestic legislation, administrative procedures, and conducting enforcement mechanisms consistent with requirements spelled out in international nonproliferation treaties.[13] These regimes, however, were not legally binding, failed to keep pace with rapid globalization and the spread of dual-use goods and technologies, and ignored the emerging role of the non-state actor in WMD proliferation.[14]

10 Richard T. Cupitt, Suzette Grillot, and Yuzo Murayama, "The Determinants of Nonproliferation Export Controls: A Membership-fee Explanation," *The Nonproliferation Review*, Vol. 8, No. 2 (June 1, 2001), p. 70; Phillip C. Saunders, "New Approaches to Nonproliferation: Supplementing or Supplanting the Regime?," *The Nonproliferation Review,* Vol. 8, No. 3 (September 1, 2001), p. 126; Matthew Bunn et al., *Preventing Black Market Trade in Nuclear Technology* (New York: Cambridge University Press, 2018).

11 NSG members adopted the dual-use guidelines in 1992 after learning about Iraq's clandestine nuclear weapons efforts, which relied heavily on acquiring goods and technologies that were not generally found on NSG control lists. In 2004, NSG members adopted a catch-all provision that permits members to block exports, even if the item does not appear on a control list if the member believes the export is headed to a nuclear weapons program.

12 David Albright and Corey Hinderstein, "Unraveling the A. Q. Khan and Future Proliferation Networks," *The Washington Quarterly,* Vol. 28, No. 2 (March 7, 2005), pp. 111–128.

13 These include the Non-Proliferation Treaty, the Chemical Weapons Convention, the Biological Weapons Convention, and the Comprehensive Test Ban Treaty.

14 William H. Tobey, "A History of United Nations Security Council Resolution 1540," in *Preventing the Proliferation of WMDs: Measuring the Success of UN Security Council Resolution 1540*, Daniel Salisbury, Andrea Viski, and Ian Stewart, eds. (Palgrave Pivot, 2018), p. 17.

By May 2003, the Bush administration began to explore options to address non-state WMD proliferation and assemble support for broader international commitments. One of the first efforts was the U.S.-led Proliferation Security Initiative (PSI), which was a non-legally binding agreement between members to accept a set of principles concerning interdicting shipments potentially related to WMD trafficking. Initially only 40 members, PSI membership now totals 105. However, as some have pointed out, although PSI improved coordination and communication between international counterproliferation efforts, it did not address several legal challenges.[15] Eventually, Bush administration officials moved to put forward a UN resolution that would mandate countries to address WMD proliferation threats—namely by criminalizing the proliferation of WMD and putting into place national export control systems. United Nations Security Council Resolution 1540, adopted in 2004, requires all member states to implement "appropriate effective" domestic rules and regulations—including export controls, border controls, physical protection of nuclear materials, and financial controls—to prevent the spread of WMD technologies to non-state actors.[16] These requirements, in theory, form a baseline level allowing states to implement country-specific UN sanctions.

U.S. Coordination and Capacity Building Efforts

Although not the focus of this report, it is important to highlight U.S. outreach, capacity-building, and other diplomatic efforts to ensure states' compliance with UNSCR 1540 goals and objectives. A key criticism of UNSCR 1540 is that although the Resolution is legally binding, it lacks an enforcement mechanism. Thus, from a governance perspective, it is incumbent on states with robust supply-side controls to assist weaker states. In the United States, for example, the State Department's *Export Control and Related Border Security Program* (EXBS) has provided technical assistance, training and outreach to more than sixty countries with varying degrees of success. The Department of Energy conducts outreach and technical assistance to help states secure materials and implement nuclear smuggling

15 Tobey, "A History of United Nations Security Council Resolution 1540."

16 "United Nations Security Council Resolution 1540," April 28, 2004.

detection and deterrence programs along borders.[17] The Department of Commerce works with foreign companies to implement rigorous corporate compliance and due diligence programs for export controls.[18]

However, this approach is still inadequate to address non-compliant and non-cooperative states. In fact, the United States has taken coercive tactics when presented with egregious issues of non-compliance. For example, the United Arab Emirates and Malaysia both implemented national export legislations in 2007 and 2010, respectively, but only after coming under threat of sanctions by the United States.

Fourteen years after the adoption of UNSCR 1540, several states continue to fall behind in implementing the Resolution's obligations.[19] According to the most recent UN report, 137 of 193 member states have put into place nuclear export control legislation, meaning more than 50 states have not done so. Only 60 states have catch-all provisions in their export control laws (i.e., rules and regulations governing goods and technologies that do not fall under an export control regime) and only 84 states have legal authorities that address transshipment (i.e., shipping goods to a third-party jurisdiction before being shipped to its final destination).[20] Vague guidance on the more than 300 requirements of the resolution, as well as concerns about the Resolution's applicability to national goals and objectives, undermine implementation efforts.[21]

Two key themes have emerged to explain states' failure to act. The first suggests that states see strategic trade controls as self-limiting and potentially harmful to their national economic and security interests. The sec-

17 For a comprehensive review of international frameworks for strengthening nuclear security, see Matthew Bunn, Nicholas Roth, and William H. Tobey, "Revitalizing Nuclear Security in an Era of Uncertainty" (Cambridge, Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2019).

18 For a discussion of the role of the private sector in WMD trafficking and current outreach and capacity-building efforts, see Robert Shaw, "The Private Sector's Role in Stopping Black-Market Nuclear Technology Networks," in *Preventing Black Market Trade in Nuclear Technology*, eds. Matthew Bunn et al. (New York: Cambridge University Press, 2018), pp. 159–184.

19 "Report of the Security Council Committee Established pursuant to Resolution 1540 (2004)" (United Nations Security Council, December 9, 2016).

20 "Report of the Security Council Committee Established pursuant to Resolution 1540 (2004)," p. 23.

21 The resolution uses the term "appropriate effective" to describe these measures and provides limited guidance about the specifics of implementation. Above all, many states which have put in place new legislation and other measures have not been seen to conduct significant export control or UN sanctions *enforcement* action against proliferation networks.

ond theme suggests that a lack of national capacity, limited capability and resources, and various bureaucratic and political constraints impede the implementation of trade controls.

In an early study of national export control systems, Cupitt et al. proposed a framework, based on an economic-rationalist perspective, to describe the conditions when states are likely to implement internationally compatible export controls.[22] The framework attempts to explain why states implement export control systems in terms of maximizing the political and economic benefits of belonging to a liberal international community. The authors conclude that resource constraints and the political costs of administering a national export control systems account for a "considerable portion of the policy variance" between countries, rather than the particular government's perception of external security threats posed by WMD-related illicit trade and proliferation.[23]

In a more recent study, Stinnett et al. discuss states' compliance with UN Security Council Resolution 1540 from two perspectives: external pressure and capacity.[24] Whereas the former perspective explains compliance as a consequence of national interest and external pressures, the capacity perspective emphasizes limitations in the technical and bureaucratic capabilities of governments.[25] In an analysis of thirty countries, the authors found significant evidence to support the limited capacity explanation for states' willingness to implement its UNSCR 1540 obligations. The authors found no support for the hypothesis that states with economies that rely heavily on exports would have greater economic incentives not to implement 1540 obligations or the hypothesis that strategic partnerships with the United States are associated with "more aggressive nonproliferation efforts."[26] These findings are generally consistent with an earlier study of UNSCR 1540

22 Cupitt, et al., "The Determinants of Nonproliferation Export Controls."

23 Cupitt, et al., p. 74.

24 Douglas M. Stinnett, Bryan R. Early, Cale Horne, and Johannes Karreth, "Complying by Denying: Explaining Why States Develop Nonproliferation Export Controls," *International Studies Perspectives*, Vol. 12, No. 3 (August 1, 2011), pp. 308–326.

25 George W. Downs, David M. Rocke, and Peter N. Barsoom, "Is the Good News about Compliance Good News about Cooperation?," *International Organization*, Vol. 50, No. 3 (1996), pp. 379–406; Abram Chayes and Antonia Handler Chayes, "On Compliance," *International Organization*, Vol. 47, No. 2 (1993), pp. 175–206.

26 Stinnett et al., "Complying by Denying," p. 323.

compliance by Fuhrmann, who finds that compliance is strongly associated with both political willingness and capacity.[27]

In addition to Resolution 1540 obligations, there are several other international agreements—both legally binding and non-legally binding—that address threats stemming from WMD-related proliferation. Several UN sanctions regimes, for example, require member states to enact measures to detect, prevent, and stop certain financial transactions, as well as implement trade restrictions related to WMD proliferation. UN Resolutions in 2006 required member states to prevent the export of nuclear, missile and military technologies to North Korea.[28] Subsequent UN Resolutions have broadened the measures against North Korea significantly to include trade embargoes on coal and other goods, financial sanctions, and maritime restrictions on North Korean shipping.[29] However, as with Resolution 1540, compliance with UN sanctions regimes and enforcement can vary significantly—even though the UN sanctions are legally binding measures.

In the case of North Korea, for example, Pyongyang has demonstrated a keen ability to exploit gaps in states' sanctions implementation. According to the March 2018 UN Panel of Experts Report, North Korea's illicit networks traded in banned goods through China, Mexico, Russia, and the Philippines, among several others.[30] They established front companies in jurisdictions like the British Virgin Islands, Australia, Hong Kong, China, and Malaysia, as well as brokering services in Australia, Angola, Egypt, Italy, and Japan.[31] To finance illegal trade and commerce—including military sales to Mozambique and Namibia and ballistic missile technology to Syria—Pyongyang's agents built banking relationships throughout China,

27 Matthew Fuhrmann, "Making 1540 Work: Achieving Universal Compliance with Nonproliferation Export Control Standards," *World Affairs*, Vol. 169, No. 3 (Winter 2007), p. 143.

28 "United Nations Security Council Resolution 1695," July 2006; "United Nations Security Council Resolution 1718," October 2006.

29 UN Security Council Resolution 2270, 2 March 2016, placed restrictions on North Korea's exports of coal and Iron. UN Security Council Resolution 2321, 30 November 2016, banned North Korean exports of copper, nickel, silver and zinc. UN Security Council Resolution 2371, 5 August 2017, banned North Korean seafood exports. UN Security Council Resolution 2375, 11 September 2017, banned textile exports and placed a cap on crude oil imports. UN Security Council Resolution 2397, 22 December 2017, strengthened previous sanctions by further restricting fuel imports and the ability of North Korean citizens to work abroad.

30 "Report of the Panel of Experts Established Pursuant to Resolution 1874," pp. 16–18.

31 "Report of the Panel of Experts Established Pursuant to Resolution 1874," pp. 22, 40.

Russia, Libya, the United Arab Emirates, and Saudi Arabia.[32] The sheer number of countries involved in these recent evasion efforts illustrate both the scope of North Korean activities and that all countries could potentially be exploited in proliferation networks.

Other multilateral commitments have dealt issues that run parallel to WMD proliferation—like proliferation financing and money laundering. Since 2012, for example, the Financial Action Task Force (FATF), which is an inter-governmental body established in 1989 that promotes the implementation of global anti-money laundering standards, has recommended that states implement targeted financial sanctions, "…to comply with United Nations Security Council resolutions relating to the prevention, suppression, and disruption of the proliferation of weapons of mass destruction and its financing."[33] Such recommendations are increasingly important as the international community turns to targeted financial and economic sanctions to punish states engaged in WMD proliferation. Much like Resolution 1540, however, international controls on the financing of proliferation are fragmented and vary widely by state.[34] Some countries, like Singapore, have extensive legislation that criminalizes the financing of proliferation, specifically. Others only implement controls based on entity lists, thus leaving room for proliferators and sanctions evaders to obfuscate payments by other means.[35]

To summarize, while there is a range of international and multilateral agreements to control the spread of WMD-related goods and technologies, they are often weak, rarely legally binding, and, in many cases, vague. Consequently, the United States has developed counterproliferation practices that seek to address these gaps that emerge beyond traditional U.S. juris-

32 "Report of the Panel of Experts Established Pursuant to Resolution 1874," p. 60.

33 "The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation" (Paris, France: Financial Action Task Force, February 2012), p. 13.

34 See, Sonia Ben Ouagrham-Gormley, "Banking on Nonproliferation," *The Nonproliferation Review*, Vol. 19, No. 2 (July 1, 2012), pp. 241–265; Nikos Passas, "Financial Controls and Counter-Proliferation of Weapons of Mass Destruction," *Case Western Reserve Journal of International Law* Vol. 44, No. 3 (March 2012), pp. 747–763; Emil Dall, Andrea Berger, and Tom Keatinge, "Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance" (London: Royal United Services Institute, June 2016).

35 For a comprehensive review and assessment of proliferation financing typologies, see Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation" (London: Project Alpha, Centre for Science and Security Studies, King's College London, October 12, 2017).

dictions. The next section describes the primary statutory authorities that criminalize WMD proliferation-related activities.

Domestic U.S. Authorities for Counterproliferation Law Enforcement

In the broadest sense, U.S. counterproliferation efforts seek to discourage interest in pursuing WMD, prevent efforts to acquire WMD or related technologies, roll back existing programs, and deter WMD use by possessor states by leveraging defense, intelligence, diplomatic, and law enforcement capabilities.[36] Although many statutes address the domestic and international security concerns of WMD proliferation, the following describes the primary criminal and civil legal authorities and regulations available to U.S. law enforcement agencies.[37]

The Atomic Energy Act (AEA). The AEA, which Congress passed in 1956 (amending the 1946 Atomic Energy Act), lays out the cornerstone policies of the United States for both civilian and military use of nuclear technologies. The Act makes anyone who "…willfully violates, attempts to violate, or conspires to violate…" its provisions subject to criminal prosecution. The Act also makes it illegal for "…for any person, inside or outside of the United States, to knowingly participate in the development of, manufacture, produce, transfer, acquire, receive, possess, import, export, or use, or possess and threaten to use, any atomic weapon." The criminal penalties are specified in 42 U.S.C, Chapter 23, section 2272. Depending on the criminal act and the magnitude of harm, penalties can range from fines up to $2 million to a life sentence in prison.

36 Although the U.S. has long lacked a unified counterproliferation policy, the concept generally refers to leveraging intelligence, defense, and law enforcement tools to disrupt, deter, and prevent WMD proliferation. In contrast, nonproliferation efforts generally rely on diplomatic, legal, and regulatory arrangements to dissuade actors from WMD acquisition and reinforce global WMD nonproliferation norms. For an early discussion of counterproliferation policy, see Ashton Carter, "How to Counter WMD," *Foreign Affairs* Vol. 83, No. 5 (September 1, 2004), pp. 72–85.

37 For an overview of U.S. nonproliferation regimes, see Mary Beth Nikitin, Paul A. Kerr, and Steven A. Hildreth, "Proliferation Control Regimes: Background and Status" (Washington, D.C.: Congressional Research Service, October 25, 2012).

The Arms Export Control Act (AECA). Enacted in June 1976, the AECA gives the president authority to control and regulate the export and import of military-related goods. Although the AECA is focused mainly on military-related trade, the Act does oblige the president to prohibit sales to any country that—after August 1977—delivers or receives "nuclear reprocessing equipment, materials, or technology to any other country" or is a "non-nuclear-weapon state which, on or after August 8, 1985, exports illegally… from the United States any material, equipment, or technology which would contribute significantly to the ability of such country to manufacture a nuclear explosive device…" The AECA makes it a crime to "…willfully, in a registration or license application or required report, make any untrue statement of a material fact or omit to state a material fact required to be stated therein or necessary to make the statements therein not misleading…" Most of these provisions are implemented through the International Traffic in Arms Regulations (ITAR). Violations of section 2278, which detail licensing and munitions list requirements, are punishable by up to a $1 million fine and twenty years in prison.

The Export Control Reform Act (ECRA). Signed in 2018 as part of the National Defense Authorization Act, the ECRA is the newest fixture of U.S. export control legislation that permanently enacts significant portions of the 1979 Export Administration Act (EAA), which had expired in 1994.[38] In addition to giving the president authorities to maintain export control lists, the Act also requires the Administration to identify and regulate "emerging and foundational technologies of concern," in addition to other licensing administration functions. Regarding enforcement, the ECRA makes it a crime for someone who "…knowingly violates or conspires to or attempts to violate any provision… or any regulation, order, or license issued thereunder…" In other words, violations of the implementing regulations carry criminal and civil penalties, which range from up to a $1 million fine and ten years in prison. The ECRA also includes civil penalties for violations, which can include fines up to $300,000 or the revocation of

38 The Export Administration Act (1979) gave the president the legal authority to implement U.S. export controls for national security reasons. Although the Act was only in force from 1979 to 1994 (with a lapse from 1984-1985), presidents since George H.W. Bush have reauthorized the law using authorities found under the International Emergency Economic Powers Act. The EAA is also one of the primary statutory authorities for the Export Administration Regulations (EAR), which articulates the list of export-controlled items. John T. Masterson, "Legal Authority Export Administration Regulations" (Washington, D.C.: U.S. Department of Commerce, Office of the Chief Counsel for Industry and Security, January 2017).

export privileges. Also, the ECRA expands law enforcement authorities for the Department of Commerce. The Agency can now use possible violations of the ECRA as a predicate offense to obtain search warrants, conduct undercover operations, conduct both domestic and foreign investigations, and make arrests. These authorities are now consistent with other law enforcement agencies, like the Federal Bureau of Investigation.

International Emergency Economic Powers Act (IEEPA). First signed in 1977, IEEPA provides the president sweeping authorities to regulate international transactions in times of national security crises. Prior to IEEPA, the president used authorities under the 1917 Trading with the Enemy Act to regulate international trade and commerce in times of national crisis. The problem, however, was that the 1917 Act was not entirely clear regarding its scope and duration.[39] Practically, IEEPA and the Trading with the Enemy Act are the same, but with one notable difference. While the United States must be in a state of war for the president to regulate trade and commerce under the Trading with the Enemy Act, the president has complete discretion to declare a national emergency under IEEPA. The only requirement is that the emergency is an "unusual and extraordinary" threat that emanates in whole or substantially outside of the United States. What exactly constitutes "unusual" or "extraordinary," however, is up for interpretation. Once the president declares a threat, he or she can investigate, regulate, or prohibit a range of transactions and economic activities with few exceptions. The exceptions primarily relate to humanitarian aid and education materials. Per the statute—not the corresponding implementing regulations—violations or conspiracy to violate IEEPA can result in criminal penalties including fines up to $1 million and up to twenty years in prison. Violating IEEPA is also a predicate offense for many financial crimes, like money laundering. This means IEEPA violations can also incur money laundering charges, which have far stiffer penalties. There are also civil penalties associated with IEEPA violations, including fines up to $250,000.

Supporting Legislation and Executive Actions. IEEPA is by far the most commonly used legal authority to impose restrictions against WMD pro-

39 Richard Nixon used the statute in 1970 to call in the National Guard to deliver mail during a postal workers' strike.

liferators—both state and non-state actors—primarily due to the flexibility and power it provides the president.[40] In 1994, for example, President Clinton signed Executive Order 12938, which declared the proliferation of WMD to be an "unusual and extraordinary" threat to the United States, and directed Federal agencies to develop policies to control exports of WMD-related goods and technologies, as well as impose sanctions on states that stockpile or use chemical or biological weapons. In 2005, President Bush expanded the scope of the executive order by imposing sanctions on foreign persons that "…have engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery…"[41] Violations of these executive orders, among many others, are governed under IEEPA penalties.

In addition to executive orders, several pieces of Congressional legislation also rely on IEEPA, AECA, and EAA (now ECRA) authorities to provide a legal basis for criminal and civil penalties. The 1996 Iran Sanctions Act (as amended), for example, specifically targets Iran's energy sector, as well as persons who export, transfer, or transship military and weapons-related goods and services. Under the Act, the President can use IEEPA authorities to impose a range of economic restrictions.

The 2010 Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) also permits the President to leverage IEEPA authorities to target Iran's banking and finance sectors. In addition to prohibiting most imports from Iran, the Act also imposes IEEPA-based restrictions—issued by the Secretary of the Treasury—that bar U.S. banks from opening correspondent accounts with any foreign financial institution that facilitate Iran's WMD or nuclear program.[42]

40 Dianne E. Rennack, "Iran: U.S. Economic Sanctions and the Authority to Lift Restriction" (Washington, D.C.: Congressional Research Service, May 10, 2018).

41 "Executive Order 13382, Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters," June 28, 2005.

42 Rennack, "Iran: U.S. Economic Sanctions and the Authority to Lift Restriction," p. 17.

Domestic U.S. Implementation and Enforcement

U.S. national authorities responsible for enforcing counterproliferation-related rules and regulations are spread across more than a dozen agencies, offices, and inter-agency organizations. Below we highlight the key agencies and offices with law enforcement authorities to investigate and prosecute WMD proliferation-related violations or with regulatory functions that may impact enforcement.

Federal Bureau of Investigation. In July 2011, the FBI established the Counterproliferation Center (CPC) to combat the spread of WMD and other technologies. As part of the agency's Counterintelligence Directorate, the CPC draws upon both intelligence and law enforcement authorities to facilitate proliferation-related investigations and operations worldwide. These include violations of the Arms Export Control Act, Export Administration Act, Trading with the Enemy Act, and the International Emergency Economic Powers Act.

Department of Homeland Security. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) is in charge of the agency's Counterproliferation Investigations Program, which is responsible for investigating and preventing "…sensitive U.S. technologies and weapons from reaching terrorists, criminal organizations and foreign adversaries." According to ICE, HSI has the broadest investigative and enforcement authorities for issues dealing with export laws. The statutory authorities include the Arms Export Control Act, the Export Administration Act, the International Economic Emergency Powers Act, as well as other statutes that deal with smuggling and trafficking.

ICE is also the steward of the inter-agency Export Enforcement Coordination Center (E2C2), which it serves as the primary coordinating hub for all federal export control-related investigations and operations. In November 2010, President Obama established the E2C2 under Executive Order 13558—largely a result of a 2006 Government Accountability Office report that highlighted several gaps and inefficiencies in U.S. export control

enforcement systems.[43] In addition to coordinating information between agencies, the E2C2 also serves to reconcile and resolve investigative and operational issues that may arise, act as the primary conduit between law enforcement and the intelligence communities, coordinate public outreach, and establish government-wide reporting and tracking databases. Participating agencies include the Departments of Commerce, Defense, Energy, Homeland Security, Justice, State, Treasury, the U.S. Postal Inspection Service, and the Office of the Director of National Intelligence.

Customs and Border Protection (CBP) provides support to the Proliferation Security Initiative (PSI)—a global effort that began in 2003 aimed at stopping the trafficking of WMD, their delivery systems, and related materials. States participating in the PSI agree to many commitments, including interdicting the transfers to and from states and non-state actors, developing mechanisms to facilitate information exchanges, and strengthening national legal authorities to facilitate interdictions. Although the State Department provides the outward facing point of contact, for its part, CBP applies its full range of enforcement and investigative authorities in support of PSI. These include targeting and analysis, inspection and detention, intelligence and information sharing, and industry outreach.

Department of Commerce. Within the Department's Bureau of Industry and Security, the Office of Export Enforcement (OEE) is responsible for investigating and prosecuting export control violations, as well as conducting industry outreach and training. The OEE also maintains stewardship of the Sentinel program, which ensures compliance by conducting end-user verification checks and educational outreach to foreign trade groups.

As part of the 2018 Export Control Reform Act, the Department of Commerce received new legal authorities to enhance its investigations and operations, including the use of undercover employees. Before the 2018 Act, the Department of Commerce had the authority to carry out general

43 The report specifically called attention to difficulties with coordinating information among agencies, due to different case management IT systems, processes, and procedures. See "Export Controls: Challenges Exist in Enforcement of an Inherently Complex System" (Washington, D.C.: United States Government Accountability Office, December 2006).

investigative activities and impose administrative sanctions and civil penalties—including denying export privileges.[44]

Department of Justice, National Security Division. The National Security Division was established in 2006 as part of the USA PATRIOT Act reform efforts to consolidate the coordination and cooperation between prosecutors and law enforcement agencies. Within the division, the Counterintelligence and Export Control Section is responsible for supervising or coordinating the prosecution of WMD proliferation-related cases that are referred by the FBI, DHS, Commerce, and other agencies.

Department of the Treasury. The Financial Crimes Enforcement Network (FinCEN), which is responsible for safeguarding the U.S. financial system, facilitates the collection, analysis, and dissemination of financial intelligence to U.S. law enforcement. Much of this intelligence is collected through regulatory reporting requirements under the Bank Secrecy Act (i.e., Currency Transaction Reports, Suspicious Activity Reports, and Reports of Foreign Bank and Financial Accounts). Although FinCEN does not possess law enforcement authorities similar to the FBI or DHS/HSI, its intelligence and analysis functions are critical to furthering counterproliferation investigations and operations. FinCEN also has the authority to make "Section 314" requests on behalf of investigators. Section 314 of the USA PATRIOT Act permits FinCEN to query U.S. financial institutions for transactional information on persons of interest for the purpose of running down leads (i.e., Section 314 requests are not a substitution for obtaining a subpoena).

The Office of Foreign Assets Control (OFAC) is responsible for implementing and administering U.S. sanctions regimes. Acting under national emergency powers authorized by the president, as well as specific sanctions legislation, OFAC has the authority to conduct civil investigations and enforcement actions against sanctions violators and provide assistance to other federal, state, and local law enforcement and intelligence agencies. Although OFAC does not investigate or prosecute criminal violations, the office works closely with law enforcement and intelligence agencies

44 United States Government Accountability Office, "Export Controls: Challenges Exist in Enforcement of an Inherently Complex System," p. 12.

to develop sanctions packages, designating particular individuals and entities for sanctions enforcement. It is often the case, for example, that OFAC relies on law enforcement and intelligence information to justify its sanctions recommendations. Also, a designation can provide the necessary legal underpinning to pursue criminal or administrative action against a violator. For example, if OFAC designates an entity under Executive Order 13382, "Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters," Federal law enforcement can pursue criminal or civil charges based on the underlying IEEPA statute.

Intelligence. While the focus of this report is on extraterritorial law enforcement, it is important to recognize the close integration and cooperation between the law enforcement and intelligence communities on matters related to export controls and WMD proliferation. The National Counterproliferation Center (NCPC), which is under the Office of the Director of National Intelligence, is the primary hub for coordinating intelligence activities to counter nuclear, chemical, and biological proliferation and their means of delivery. The NCPC also acts as a critical interface with U.S. law enforcement agencies. Other intelligence agencies and offices with counterproliferation missions that closely coordinate with law enforcement include National Security Agency, S2G (counterproliferation); Central Intelligence Agency, Strategic Interdiction Group; and Defense Intelligence Agency, Defense Counterproliferation.

Summary

In addition to the diplomatic initiatives to curb international demand for WMD and reinforce nonproliferation norms, supply-side approaches have remained a staple of U.S. efforts to stem the spread of WMD proliferation-sensitive goods and technologies. In general, U.S. law enforcement agencies—with support from intelligence and diplomatic agencies—share the responsibility for investigating and prosecuting violations of U.S. WMD-related export controls.

While the United States continues to be a global leader in terms of its political and legal commitments to counterproliferation, U.S. enforcement

efforts are complex and fragmented. As illustrated above, investigations and operations are spread over several federal agencies. In some cases, there is considerable overlap between agencies. The FBI and DHS Homeland Security Investigations, for example, share the same legal authorities to investigate export control violations. Although inter-agency groups, like the Export Enforcement Coordination Center, are meant to avoid overlap and duplication, technological, bureaucratic, and sometimes legal hurdles prevent proper coordination and collaboration. A 2006 report by the Government Accountability Office specifically highlighted several impediments to greater collaboration and information sharing, like differences in case management and IT systems.[45] Unfortunately, few of these issues have been adequately addressed.[46]

Outside of the United States, there are clear disparities in national approaches, translating into a patchwork landscape of supply-side controls. While UNSCR 1540 obliges all states to put in place national export control systems, among other requirements, the resolution provides significant leeway for each state to determine its system of national legislation, implementing authorities, and priorities. From a U.S. enforcement perspective, what happens when entities violate U.S. domestic law in foreign jurisdictions? The next section details the scope and implications of these jurisdictional hurdles regarding U.S. counterproliferation law enforcement.

45 United States Government Accountability Office, "Export Controls: Challenges Exist in Enforcement of an Inherently Complex System."

46 Personal interview with former DHS law enforcement official, February 2018.

Section 2: Overseas Counterproliferation Investigations and Operations

Law enforcement counterproliferation activities generally entail some level of coordination and cooperation with foreign governments, mainly due to the transnational nature of illicit procurement. This section considers the activities and legal tools that the U.S. government has deployed in its efforts to conduct export enforcement actions overseas. It considers the U.S. approaches to the jurisdictional challenge, extraterritorial counterproliferation operations, and actions at the nexus between law enforcement and regulation. Before considering these challenges and implications, the section begins by outlining the U.S. resources available to assist in these transnational investigations and enforcement operations.

Most U.S. law enforcement agencies directly involved in counterproliferation maintain an overseas presence in order to facilitate coordination with the host government. The U.S. Department of Commerce, for example, maintains Export Control Officers (ECOs) in seven foreign jurisdictions to support end-user verification programs, as well as industry outreach and training.[47] In 2015, State Department and Department of Commerce officials conducted more than 1,000 end-user verifications in 55 countries.[48] The Department of Homeland Security's HSI maintains 66 offices in 49 countries as of 2017—although these resources are generally in support of broader Immigration and Customs Enforcement missions.[49] Similarly,

47 This includes offices in Beijing and Hong Kong, China; Abu Dhabi, UAE; New Delhi, India; Singapore; and Frankfurt, Germany; a post in Moscow is currently vacant. "Export Control Officer Program (ECO)," Bureau of Industry and Security, U.S. Department of Commerce, https://www.bis.doc.gov/index.php/enforcement/oea/eco, (accessed February 11, 2019).

48 Kevin J. Kurland, "End-Use Monitoring and Effective Export Compliance," (November 1, 2015), https://www.bis.doc.gov/index.php/documents/update-2015-presentations/1344-civil-military-evaluation-end-user-verification-kurland/file (accessed February 11, 2019). For military-related items, the Department of State conducts end-use checks through the BLUE LANTERN program. Since 1990, there have been over 14,000 checks conducted in more than 100 countries. See Office of Defense Trade Controls Policy, Directorate of Defense Trade Controls, U.S. Department of State, "Blue Lantern End-Use Monitoring Program," (October 30, 2016), https://www.bis.doc.gov/index.php/documents/pdfs/1588-end-user-verification-blue-lantern/file (accessed February 11, 2019).

49 Thomas D. Homan, "Statement of Thomas D. Homan, Acting Director, U.S. Immigration and Customs Enforcement, Department of Homeland Security," (June 13, 2017), https://www.ice.gov/sites/default/files/documents/Speech/2017/170613homan.pdf (accessed February 11, 2019).

the FBI staffs 64 legal attaché offices and more than a dozen smaller offices, which provide coverage to over 200 foreign territories.[50]

According to one former law enforcement official, an overseas presence facilitates robust liaison relationships with local law enforcement and intelligence and is critical to ensuring successful counterproliferation investigations and operations.[51] One commonly used mechanism to coordinate international law enforcement efforts is INTERPOL—an international law enforcement organization with 192 member countries. With mission areas in anti-trafficking in illicit goods and CBRNE terrorism prevention, INTERPOL facilitates legal assistance, conducts capacity-building efforts, and raises awareness of proliferation-related dangers. In many cases, the United States requests an INTERPOL "Red Notice" regarding persons trafficking in WMD-related goods and technologies.[52] These notices convey relevant information about persons wanted by a member state, as well as restrict the individual's ability to travel internationally and are considered the closest instrument to an international arrest warrant.

While liaison efforts are often *ad hoc* or informal arrangements between U.S. and foreign law enforcement agencies, or over specific investigations, there are also several legal agreements to help ensure due process and reciprocity between jurisdictions.[53] For example, the United States currently has extradition treaties in place with over 100 countries.[54] Having an extradition treaty in place, however, does not guarantee legal reciprocity, and in many cases, extradition treaties are insufficient to ensure cooperation. To supplement these treaties, the United States relies on several bilateral agreements that establish rules for each party to the agreement to exchange evidence and information in criminal and civil matters. As of 2017, the United States has approximately 50 bilateral Mutual Legal Assistance Treaties (MLATs) and Agreements (MLAAs), the contents of which

50 "Overseas Offices," Federal Bureau of Investigation, May 3, 2016, https://www.fbi.gov/contact-us/legal-attache-offices (accessed February 11, 2019).

51 Personal interview with former DHS law enforcement official.

52 For additional information about Red Notices, see "Red Notices," INTERPOL, https://www.interpol.int/INTERPOL-expertise/Notices/Red-Notices (accessed September 24, 2018).

53 Charles Doyle, "Extraterritorial Application of American Criminal Law" (Washington, D.C.: Congressional Research Service, October 31, 2016), p. 26.

54 Guardian US interactive team, "A Guardian Guide to Extradition," *The Guardian*, July 2, 2013, http://www.theguardian.com/world/interactive/2013/jul/02/guardian-guide-extradition-interactive (accessed February 11, 2019).

vary between countries, but place obligations on states to assist in criminal investigations and prosecutions.[55] In most cases, these agreements rely on the principle of "dual-criminality," meaning an individual can be extradited from one country to stand trial for breaking U.S. laws only if a similar law exists in the extraditing country.

In addition to MLATs, the United States also has approximately eighty Customs Mutual Assistance Agreements (CMAAs) in place. These legal agreements, which are based upon a model developed by the World Customs Organization (WCO) and negotiated bilaterally, allow for the "exchange of information, intelligence, and documents that will ultimately assist countries in the prevention and investigation of customs offenses."[56] Although the CMAAs allow for information sharing, they "do not guarantee that U.S. law enforcement will have access to foreign persons, ports, and facilities."[57]

Several other arrangements allow for the exchange and sharing of information that may be relevant to counterproliferation investigations and operations. Concerning financial information, for example, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has several Memoranda of Understanding (MOU) to facilitate the sharing of financial intelligence between the United States and other countries' financial intelligence units (FIUs).[58] The United States is also a member of the Egmont Group, a body consisting of over 150 FIUs from different countries, which seeks to facilitate information exchange at the operational level per a set of principles and rules approved in 2013.[59] In the past, however, law enforcement has been reluctant to use these mechanisms—especially in "unfriendly jurisdictions"—for fear of giving a "tip-off" to the target of the investigation or operation.

---

55 "Treaties and Agreements," U.S. Department of State, https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm (accessed August 28, 2018).

56 "Model Bilateral Agreement on Mutual Administrative Assistance in Customs Matters" (World Customs Organization, June 2004); "Customs Mutual Assistance Agreements (CMAA)," U.S. Customs and Border Protection, https://www.cbp.gov/border-security/international-initiatives/international-agreements/cmaa (accessed August 28, 2018).

57 "Export Controls: Proposed Reforms Create Opportunities to Address Enforcement Challenges" (Washington, D.C.: Government Accountability Office, March 2012), p. 22.

58 As of 2016, this included MOUs of exchange of letters with around 50 countries. "International Narcotics Control Strategy Report, Vol. II Money Laundering and Financial Crimes" (U.S. Department of State, March 2016), pp. 20–21.

59 "Principles for Information Exchange Between Financial Intelligence Units" (Egmont Group, July 2013).

As noted above, these mechanisms facilitate *law enforcement* efforts for the United States around the world and supplement the intelligence operations, diplomatic initiatives, and the work of various international bodies dedicated to preventing the proliferation of weapons of mass destruction and their delivery systems.

Counterproliferation and the Challenge of Jurisdiction

Perhaps the single biggest impediment to successful counterproliferation law enforcement is having to contend with the political and legal challenges of foreign jurisdictions. The jurisdictional challenge stems from the basic accepted principle of sovereignty—meaning states have the right to manage their internal affairs in accordance with their laws, norms, and customs. From the perspective of accepted international legal norms, it is generally not possible (or accepted) for one state to impose its domestic law on entities inside another state. Thus, pursuing a counterproliferation policy that addresses the transnational nature of illicit WMD procurement becomes fraught with jurisdictional challenges. Often, these challenges put elements within an illicit procurement network out of jurisdictional reach. Even when states are willing to cooperate, however, differences in national legal systems and norms can frustrate investigations and prosecutions.

Furthermore, illicit networks are adaptive entities and have been known to base their operations on assessments of local legal, regulatory, and political risk—a concept known as "jurisdictional arbitrage."[60] Savvy proliferators will deliberately base themselves in jurisdictions where the risk of detection or prosecution is low. A.Q. Khan's illicit activities, for example, illustrate how jurisdictional shopping—in Malaysia, Turkey, South Africa, and the United Arab Emirates—can frustrate law enforcement efforts.

60 Phil Williams, "Transnational Criminal Networks," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, eds. John Arquilla and David Ronfeldt, 2001; Aaron Arnold, "A Resilience Framework for Understanding Illicit Nuclear Procurement Networks," *Strategic Trade Review* Vol. 3, No. 4 (Spring 2017), pp. 3–23.

Nodes out of Reach: Nicholas Kaiga

In October 2012, the U.S. Department of Justice charged Belgian national Nicholas Kaiga with export violations following a multi-year undercover investigation. According to court records, Kaiga conspired with an unnamed Iranian individual to procure export-controlled aluminum tubes from the United States. The Iranian counterpart operated front companies in the United Arab Emirates (UAE) and Malaysia, which Kaiga used to transship the goods to Iran.

Although U.S. law enforcement effectively employed undercover methods to ensnare Brussels-based Kaiga and disrupt his illicit activities, U.S. law enforcement was unable to conduct enforcement action against the Iranian elements of the network located in the UAE and Malaysia. The individual controlling the UAE and Malaysian companies, which had a limited footprint in the UAE and used a virtual office in Kuala Lumpur, appears to have been based in Iran. This case highlights the challenge of taking out nodes in proliferation networks in multi-jurisdictional law enforcement operations, and particularly when proliferators establish front companies in jurisdictions in which they are not physically based. The inability to address these nodes limits the overall effectiveness of the law enforcement actions and can leave pathways for the procurement network to reconstitute itself.

Differing Laws and Legal Systems: Gotthard Lerch on Trial

In October 2008, a German court convicted and sentenced Swiss national Gotthard Lerch to more than five years in prison for his participation in A.Q. Khan's nuclear proliferation network. According to the plea agreement, between 1999 and 2003, Lerch illegally procured and transshipped export-controlled vacuum pumps to Libya. Although Switzerland extradited Lerch to Germany in 2004, the extradition arrangements between Switzerland and Germany created several prosecutorial challenges that dragged on for four years.[1]

In particular, Switzerland's legal assistance treaty with Germany prohibited extradition for the prosecution of crimes that Switzerland does not also outlaw. German prosecutors wished to charge Lerch with one count of treason and two counts of export violations. At the time, however, Swiss law defined treason differently from German law—meaning Lerch could not be charged with this crime under Swiss law. German authorities were also forced to drop other serious charges involving the sale of nuclear technology because CIA and British intelligence refused to share relevant information with prosecutors. Moreover, Malaysia and South Africa refused to send associates of Lerch to testify against him. In 2008, Germany finally prosecuted Lerch for minor violations and sentenced him to time served.

1 Peter Crail, "Germany Convicts Khan Associate," *Arms Control Today*, November 4, 2008, https://www.armscontrol.org/print/3417 (accessed February 11, 2019); Leonard S. Spector and Egle Murauskaite, "Countering Nuclear Commodity Smuggling: A System of Systems" (James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey, March 2014), p. 142.

Shopping for Jurisdiction: Hub Selection in the A.Q. Khan Network

Seeking to fulfill a deal struck with Libya in 1997 to provide a full gas centrifuge plant for uranium enrichment, the A.Q. Khan network looked to expand its manufacturing operations in the early 2000s. Khan eventually settled on a factory in Malaysia to manufacture key components because of Malaysia's weak export control systems and lack of enforcement, as well as other favorable political and economic factors. The plant would eventually send tens of thousands of machined centrifuge parts to Libya, some of which international partners interdicted on the vessel, *BBC China*, in 2003—an event which signaled the beginning of the end of the network's activities.

Before Malaysia, Khan rejected a number of options. Dubai—a laxly regulated environment where Khan located his central transshipment hub—was dismissed because of the lack of a skilled workforce, and because of concern that importing labor and applying for work permits would raise government interest.[1] Turkey was also considered, but also dismissed because of a lack of skilled labor.[2] A third location, South Africa, was dismissed because the country's history with nuclear weapons meant that imports of specialty metals would raise concerns in exporting countries.[3]

Ultimately, Malaysia had many attributes making it an attractive legal jurisdiction for the operation—most notably, limited export control legislation and enforcement.[4] Bukhari Sayed Abu Tahir, Khan's right-hand man, also had personal and political connections to Malaysia. He "mixed with Malaysia's elite" and grew close to Kamaluddin Abdullah, the son of the Malaysian Prime Minister.[5] More broadly, Malaysia's emergence as a key manufacturing hub for various industries, alongside limited oversight, meant that imports of advanced machine tools and metals would not raise red flags in exporting states.

---

1 Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (New York: Free Press, 2014), p. 241.

2 Collins and Frantz, p. 241.

3 Collins and Frantz, p. 261.

4 As a former Malaysian official has noted, the Khan network's activities did not breach Malaysian law. M. S. A. Kareem, "Implementation and Enforcement of Strategic Trade Controls in Malaysia," *Strategic Trade Review* Vol. 2, No. 2 (2016), p. 108.

5 Albright, *Peddling Peril*, p. 134.

U.S. Legal Dimensions of Extraterritoriality

Given the transnational nature of illicit procurement, at what point does the United States consider entities and property not located within the United States within the bounds of U.S. law? International legal norms dictate interpretations of jurisdiction that can vary considerably, especially concerning extraterritorial law enforcement. Most countries base their interpretation of jurisdiction on one or more of four general principles. The first principle defines jurisdiction in terms of its geographic territory.[61] Over the last several decades, however, economic globalization and the rise of international non-governmental organizations have reduced the relevance of a territory-oriented principle of jurisdiction in most cases.[62] The most commonly adopted principle is the nationality principle—meaning states base jurisdiction on nationality rather than territory. Some countries, like the United States and Canada, have interpreted the nationality principle in a rather broad context to include citizens, companies, *and* property under its jurisdiction. This includes foreign companies that are owned or operated by U.S. entities, but otherwise located abroad, as well as companies that may only be partially owned by U.S. entities.

The last two legal dimensions of jurisdiction are the protective and universal principles. The protective principle is based on the right of a sovereign state to protect its economic and security interests.[63] In this respect, claiming extraterritorial jurisdiction is consistent with international legal norms, but is substantively and arbitrarily defined by each state in terms of what constitutes a threat. Lastly, states may claim extraterritorial jurisdiction in order to enforce universal rights. This principle is mainly concerned with state violations of international law on slavery, piracy, and certain human rights violations.

61 Hans Kelsen, *General Theory of Law and State* (Clark, N.J.: The Lawbook Exchange, Ltd., 1945), p. 208.

62 Kern Alexander, *Economic Sanctions Law and Public Policy* (London: Palgrave Macmillan, 2009), p. 68; Anne-Marie Slaughter, "The Real New World Order," *Foreign Affairs*, September 1, 1997, https://www.foreignaffairs.com/articles/1997-09-01/real-new-world-order (accessed February 11, 2019).

63 Alexander, *Economic Sanctions Law and Public Policy*, p. 85.

Problems quickly emerge, however, when a citizen in one country violates the law or threatens the security and safety of nationals in a foreign country. Under these circumstances, international norms have generally held that the extraterritorial application of the law must be through the consent of the state (i.e., the foreign jurisdiction). In practice, states give consent through multilateral or bilateral extradition agreements. Another issue arises when jurisdictional claims by one state create confusing or contradictory obligations for an individual or company headquartered in a foreign country. In other words, what happens when complying with one state's laws comes into conflict with another state's domestic laws?[64]

Between 1977 and 2001, several fundamental changes to domestic rules and regulations greatly expanded the jurisdictional reach of U.S. authorities to target overseas proliferators. In 1979, for example, Congress expanded the reach of the Export Administration Act, giving the president authority to include "persons subject to the *jurisdiction* of the United States." Because Congress failed to specify its intent as to what jurisdiction entailed, presidents have subsequently interpreted the statute broadly to include property.[65]

One of the first tests of this interpretation came in December 1981, when President Ronald Reagan attempted to slow Russia's progress on its Siberian natural gas pipeline by restricting American exports and re-exports

64 The Bank of Nova Scotia is a Canadian-registered bank headquartered in Toronto, Canada, with more than 1,200 global branches. In March 1983, the Southern District Court of Florida issued the bank's Miami branch a series of grand jury subpoenas for records held at the bank's offices in the Grand Cayman Islands as part of a tax evasion and drug trafficking investigation. A month later, the bank filed a motion to quash the subpoena in the district court, asserting that if it complied with the subpoena, it would violate the secrecy laws of the Bahamas and the Cayman Islands. Throughout the appeals process, the United States fined Bank of Nova Scotia more than $2 million for noncompliance with the subpoena. In United States v. Bank of Nova Scotia, the Eleventh Circuit upheld the $2 million fine against the bank. According to the U.S. Attorneys' Manual, "Since the use of unilateral compulsory measures can adversely affect the law enforcement relationship with the foreign country, all federal prosecutors must obtain written approval through OIA before issuing any subpoenas to persons or entities in the United States for records located abroad." See, "U.S. Attorneys' Manual, Section 279, Para. B. Bank of Nova Scotia Subpoenas" (U.S. Department of Justice), https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas (accessed August 29, 2018).

65 Edward Solensky Jr., "The President's International Emergency Economic Powers after Regan v. Wald: An Unchecked Proliferation of Authority Note," *Syracuse Journal of International Law and Commerce*, Vol. 12 (1986), p. 126.

of goods and services related to oil and gas production.[66] The pipeline, which was scheduled to supply Western Europe's energy requirements, was a politically contentious issue because it threatened to undermine the U.S. role in the region. Under the rule, Reagan banned all U.S. goods and services relating to the pipeline for export or re-export to the then-Soviet Union. Unlike previous export restrictions, however, this executive order also assumed jurisdiction over American goods already overseas or already under contract.[67] Many U.S. allies saw this jurisdictional expansion as over-reach and swiftly moved to protect their economic and national interests. In 1982, for example, the French government ordered its largest oil and natural gas manufacturers to proceed with shipments in direct violations of U.S. sanctions—mainly as a protest to America's extraterritorial application of its domestic law.[68] Amidst a rising tide of protests from critical economic partners, President Reagan rolled back the extraterritorial dimensions of the sanctions.[69]

The most significant changes to U.S. extraterritorial policy occurred after the September 11, 2001 terrorist attacks. Congressional leaders determined that amendments to existing rules and regulations could help address jurisdictional gaps, especially when dealing with terrorist financing. The U.S. Department of the Treasury would later use these new authorities against

66 "Pipeline Machismo," *The New York Times*, September 1, 1982, http://www.nytimes.com/1982/09/01/opinion/pipeline-machismo.html (accessed February 11, 2019); Ronald Reagan, "Statement on U.S. Measures Taken Against the Soviet Union Concerning Its Involvement in Poland," Press Release (December 29, 1981), Ronald Reagan Presidential Library and Museum, https://www.reaganlibrary.gov/research/speeches/122981m (accessed February 11, 2019).

67 Gary H. Perlow, "Taking Peacetime Trade Sanctions to the Limit: The Soviet Pipeline Embargo," *Case Western Reserve Journal of International Law*, Vol. 15, No. 2 (1983); A. V. Lowe, "Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, 1980," *The American Journal of International Law*, Vol. 75, No. 2 (1981), pp. 257–282.

68 Bernard Gwertzman, "U.S. to Penalize Those Who Aid Siberian Pipeline," *The New York Times*, August 26, 1982, http://www.nytimes.com/1982/08/26/business/us-to-penalize-those-who-aid-siberian-pipeline.html (accessed February 11, 2019).

69 A similar test occurred in the mid-1990s when Congress enacted the Cuban Liberty and Democratic Solidarity (Libertad) Act— also known as the Helms-Burton Act. The legislation expanded the United States' long-standing economic sanctions and embargoes against Cuba by providing legal remedies for U.S. citizens who had property confiscated by Cuba. Under the Act, U.S. citizens are permitted legal redress against any foreign company trafficking in property confiscated by Cuba. The Act also allows the president to impose sanctions against foreign entities that trade with Cuba. Almost immediately countries condemned the Act as an aggressive expansion of extraterritoriality and resulted in many states enacting national "blocking" regulations to protect their domestic companies from U.S. extraterritoriality. In 1996, for example, the European Council passed Council Regulation 2271, which declares the extraterritorial provisions of the Helms-Burton Act to be unenforceable within the E.U. Recently, the EC updated this statute in order to counteract the effects of U.S. secondary sanctions against E.U. companies after the United States unilaterally withdrew from the Joint Comprehensive Plan of Action. See, Suzanne Katzenstein, "Dollar Unilateralism: The New Frontline of National Security," *Indiana Law Journal* 90 (2015): 293–352.

banks and other financial institutions involved in sanctions violations and WMD proliferation. First, Sections 311, 312, and 313 of the USA PATRIOT Act expanded enforcement agencies' ability to enforce U.S. rules and regulations indirectly. Section 311, for example, gives authority to the Treasury Department to designate a foreign country (or entity) as a "jurisdiction of primary money laundering concern." Once designated, the Treasury Department can impose any number of special measures, to include requiring U.S. banks to conduct enhanced due diligence of its customers' accounts and transactions or even restrict banks from opening or maintaining a foreign financial institutions' correspondent account.[70]

Finally, the USA PATRIOT Act amended IEEPA language to extend jurisdiction to both people and property. As previously mentioned, most countries adhere to the principle of nationality when determining jurisdiction, which for all intents and purposes, pertains to individuals and companies. Extending this to include property is a much broader interpretation, which gives authorities significant leverage over foreign institutions trading with U.S. banks and businesses.[71]

U.S. Extraterritorial Counterproliferation Operations

When cooperative efforts fail or are not feasible for political or security reasons, U.S. law enforcement agencies have employed a number of tools to target overseas proliferators. The following describes the scope of these methods and how law enforcement agencies have historically used them.

70 Correspondent banking is when one bank carries out transactions on behalf of another bank—usually a foreign bank. These relationships allow a customer at one institution to quickly send a payment to a foreign bank. For example, Bank of China would settle a payment from an account holder at Bank of New York by debiting Bank of New York's correspondent account and credit its client. If, say, Bank of China and Bank of New York did not have a correspondent relationship, the transaction might need to go through multiple correspondent accounts at different banks (i.e., a correspondent network). A correspondent account, then, is a bank's account at a different institution.

71 After Russia annexed Crimea in March 2014, Washington moved to sanction certain entities that undermined Ukraine's democratic processes. Previously, Treasury's Office of Foreign Assets Control adhered to the "fifty percent rule" when determining individual ownership and interest in a foreign company that is subject to sanctions. That is, any company that is more than fifty percent owned by a sanctioned individual is also sanctioned. New guidance issued in 2014, however, significantly expanded this scope by using an aggregate standard. Thus, if the *aggregate* ownership of any company is more than fifty percent owned by sanctioned entities, that company is also sanctioned. Office of Foreign Assets Control, "Ukraine/Russia-related Sanctions Programs" (U.S. Department of the Treasury, June 16, 2016).

Notably, this section explores U.S. operations to counter proliferation networks through undercover, sting, and lure operations, and through information operations.

Undercover, Sting, and Lure Operations. Seeking extradition for violations of U.S. federal law can be a complicated process, as states may lack sufficient legal frameworks or political will to effectuate extradition proceedings with the United States. In such cases, the U.S. law enforcement agencies resort to alternative methods. Since the 1980s, federal law enforcement has used varying degrees of deception to investigate and prosecute overseas illicit procurement networks.[72]

In such cases, sting and undercover operations have become commonplace investigative tools to build criminal cases. Although the use and definition of undercover operations can vary by agency, the FBI defines its undercover activities as "…any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI."[73] It is important to note, however, that not all Federal law enforcement agencies have the legal authority to conduct undercover or sting operations. The Department of Commerce only recently received statutory authority to conduct undercover operations in support of their mission as part of the 2018 Export Control Reform Act.

Obtaining an indictment against an overseas procurement agent is not necessarily a simple or straightforward process. U.S. prosecutors are often reluctant to indict those overseas for many reasons, but most common among those are the low likelihood of the subject being extradited to the United States and the low likelihood of obtaining a conviction if the subject is extradited. In some cases, lack of expertise or knowledge about

72 See, Gaylord Shaw and William C. Rempel, "Billion-Dollar Iran Arms Search Spans U.S., Globe: Even Pentagon Penetrated by Massive Effort," *Los Angeles Times*, August 4, 1985.

73 "The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations" (U.S. Department of Justice, 2013), p. 1; Graeme R. Newman, "Sting Operations" (U.S. Department of Justice, Office of Community Oriented Policing Services, October 2007), p. 3. In some overseas jurisdictions, like Germany, most types of sting and undercover operations are considered illegal due to entrapment concerns. For an intriguing insider's glimpse at international undercover operations, see John Shiffman, *Operation Shakespeare: The True Story of an Elite International Sting* (New York: Simon & Schuster, 2014).

the case contributed to the decision not to pursue an indictment. As one law enforcement official noted, the bureaucratic process of an indictment is cumbersome, and "un-indicting" someone is a far more difficult and time-intensive process.[74] In other cases, political decisions can affect the decision to indict.

The Sting: Jiang Guanghou Yan

Jiang Guanghou Yan pled guilty in March 2016 for intentionally trafficking in fraudulent goods.[1] Yan worked as a representative in China for a Shenzhen-based company, HK Potential. The investigation began in 2012 when industry sources provided DHS investigators information about suspicious inquiries that Yan had made during a trade show. Specifically, Yan expressed interest in the processes and techniques certain manufacturers use to detect counterfeit integrated circuits.

Eventually, law enforcement agents, acting in an undercover capacity, purchased and received several orders of integrated circuits that Yan knowingly altered to appear as if they were a higher grade. By July 2015, Yan had attempted to procure export-controlled military-grade integrated circuits, used in a variety of military applications, for shipment to China— even offering to replace the stolen parts with counterfeit parts. Yan was eventually taken into custody in December 2015 when he traveled to the United States in order to finalize the transaction. The case represents a typical undercover sting operation, targeting an individual overseas.

1 "Actual Investigations of Export Control and Antiboycott Violations" (U.S. Department of Commerce, Bureau of Industry and Security, January 2017), p. 48.

Once law enforcement authorities have obtained enough information to pursue an indictment, the next step is to secure an arrest, which is not always feasible if the subject is located overseas. In counterproliferation-re-

74 Personal interview with former DHS law enforcement official.

lated investigations, lure operations and INTERPOL Red Notices are common methods when hurdles to seeking extradition seem insurmountable.

As previously mentioned, Red Notices are the closest legal instrument to an international arrest warrant and can be distributed as widely or as narrowly as needed. This flexibility can help reduce concerns about ad-

Prisoner Swaps, Nuclear Deals, and Politics

In early 2016, the Department of Justice released seven Iranian prisoners held in the United States and dropped charges against 14 others.[1] Of those released, one Iranian was incarcerated for running a network responsible for procuring U.S.-manufactured microelectronics for use in surface-to-air missiles. Another was serving eight years for conspiracy to supply Iran with satellite technology. Most of the cases that prosecutors dropped, however, involved suspects located overseas, in particular in Iran. One of the Iranians was Seyed Jamili, who procured more than 1,000 pressure transducers for Iran's nuclear program through a Chinese intermediary.[2] The intermediary, Sihai Cheng, is currently serving a nine-year prison sentence for IEEPA violations.[3]

The release of these prisoners and dropping of these cases show how high-level political considerations can impact export enforcement. While the Obama administration claimed the move was to secure the release of American prisoners in Iran, others chided the decision as politically-motivated and connected to securing the Joint Comprehensive Plan of Action (JCPOA)—the agreement between Iran and world powers, which limited Iran's nuclear program in exchange for sanctions relief.

1 Josh Meyer, "Obama's Hidden Iran Deal Giveaway," Politico, April 24, 2017, http://politi.co/2p8Grla (accessed February 11, 2019).

2 A pressure transducer—also referred to as a pressure transmitter—converts pressure into an analog electrical signal. Highly calibrated pressure transducers are key centrifuge components for the enrichment process.

3 Milton J. Valencia, "Chinese Man's Lawyers Say Iran Deal Left Client Caught in Middle," *Boston Globe*, January 27, 2016.

versarial governments providing a "tip-off" warning to the fugitive. If a foreign government arrests a fugitive pursuant to an INTERPOL Red Note, it is incumbent on the U.S. prosecutor to secure the required extradition documents for that specific jurisdiction, per existing treaties or that country's domestic law.

In some cases, such as that of David Levick, an Australian individual who allegedly exported U.S. goods to Iran via Malaysian intermediaries, Australia's extradition treaty with the United States did not cover the crimes with which he was charged.[75] In another example, the U.S. extradition treaty with Singapore, which came into force more than eighty years ago in 1935—when Singapore was still part of the British Empire and before the advent of nuclear weapons or ballistic missiles—does very little to address export control concerns.[76] Where national laws do not include provisions for export violations, other charges such as conspiracy or falsifying documents may be used. Having to find alternative criminal charges to facilitate cooperation is quite common in proliferation-related cases. One of the main reasons is that many of the U.S. export control laws are authorized under presidential national emergency powers, which is technically a temporary authorization. Often, foreign jurisdictions lack similar laws or are reluctant to cooperate with U.S. extradition requests based on presidential emergency authorizations.

In other cases, such as the Iranian cases described in the box below, the government of the arrested person has marshalled significant political arguments and even issued veiled threats, communicated both publicly and privately, against the extraditing governments (e.g., Thailand, the UK and Hong Kong—all of which have extradition treaties in place with the United States) in order to try and prevent extradition. Those in the crosshairs often view strategic trade controls and sanctions as politically motivated. As one former enforcement official noted, law enforcement in these areas is "more political than traditional enforcement areas."[77]

75 Erich Ferrari, "David Levick Indicted for Criminal Export Violations," *SanctionLaw*, March 2, 2012, https://sanctionlaw.com/david-levick-indicted-for-criminal-export-violations/ (accessed February 11, 2019).

76 United States, Singapore, "Singapore International Extradition Treaty with the United States," June 24, 1935, https://goo.gl/JiEYwj (accessed February 11, 2019); "Export Controls: Proposed Reforms Create Opportunities to Address Enforcement Challenges."

77 Personal interview with former DHS law enforcement official.

Late 2000s Iranian Extradition Cases

A series of cases involving Iranian nationals in the mid-to-late 2000s provide some insights into the challenges of extraditions. During this period, Iranian procurement networks were actively seeking military-grade goods and technologies.

- Jamshid Ghassemi, a high-ranking Iranian Air Force official, was arrested in Thailand in 2006 for attempting to procure accelerometers for use in missile guidance systems. Ghassemi's defense reportedly made three arguments for his release: that U.S. extradition documents were filed too late, that Ghassemi would face torture to reveal Iranian military secrets in the United States, and that the U.S.-Thailand extradition treaty exempts "military offenses."[1] Ghassemi was released in September 2008 after Thailand denied the extradition request.
- Nosratollah Tajik, a former Iranian ambassador to Jordan, faced extradition from the United Kingdom to the United States following a U.S. sting operation during which he sought to export U.S. night vision goggles to Iran. UK authorities approved the

1 John Pomfret, "U.S. Presses Thailand to Hand over Accused Russian Arms Dealer," *The Washington Post*, August 19, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/08/19/AR2010081906034.html (accessed February 11, 2019).

When formal extradition efforts fail, U.S. law enforcement will often use lure operations against targets in unfriendly states. The U.S. Attorneys' Manual defines a lure operation as using "…subterfuge to entice a criminal defendant to leave a foreign country so that he or she can be arrested in the United States, in international waters or airspace, or in a third country for

extradition request in 2007. However, the United States allegedly did not respond until 2011. Tajik appealed the order because the process had taken too long and won in 2012.[2] It is important to note that during the extradition process, the UK government expressed strong concerns that Tajik's extradition could lead to Iranian retributions against UK diplomatic staff.[3]

- A third individual, Yousef Boushvash, was arrested in Hong Kong in 2007 following a U.S. sting operation in which he attempted to procure U.S.-origin fighter aircraft parts for Iran.[4] In 2008, a Hong Kong government official noted that the authority to extradite Boushvash to the United States had been withdrawn "per instructions from the central government of the People's Republic of China."[5] After release by the Hong Kong authorities, Boushvash disappeared and managed to evade U.S. authorities and an INTERPOL arrest warrant.

2 Terri Judd, "Former High Ranking Iranian Diplomat Nosratollah Tajik Avoids Extradition to US," *The Independent*, November 27, 2012, https://www.independent.co.uk/news/uk/crime/former-high-ranking-iranian-diplomat-nosratollah-tajik-avoids-extradition-to-us-8360080.html (accessed February 11, 2019).

3 American Embassy in London, "Iran: UK Intends to Go Forward on Tajik Extradition but Concerned About Safety of Its Tehran Embassy" (Department of State, June 2008), http://wikileaks.wikimee.org/cable/2008/06/08LONDON1580.html (accessed February 11, 2019). Indeed, these concerns may have been credible given the storming of the UK's mission in Tehran in 2011 by protestors.

4 Mark Hosenball, "Back on the Black Market," *Newsweek*, June 21, 2008, http://www.newsweek.com/back-black-market-90731 (accessed February 11, 2019).

5 Mark Hosenball, "U.S. Faces Setbacks on Blocking Arms Sales to Iran," *Newsweek*, October 7, 2008, http://www.newsweek.com/us-faces-setbacks-blocking-arms-sales-iran-92237 (accessed February 11, 2019).

subsequent extradition…"[78] Such lure operations have proven successful in a number of counterproliferation-related investigations.

Interestingly, while lure operations are a preferred method of bringing a fugitive into custody when legal extradition arrangements are unavailable, the U.S. Department of Justice maintains the legal opinion that extraterritorial law enforcement activities are not prohibited even if they contravene international customary law. The FBI, for example, could make an arrest in a foreign jurisdiction without the consent of government authorities in that

78 U.S. Department of Justice, "United States Attorneys' Manual," 2018, secs. 9–15.630.

jurisdiction.[79] Before this 1989 legal memorandum, the Justice Department considered such action to be an "…invasion of sovereignty for one country to carry out law enforcement activities within another country without that country's consent."[80] Such cases, however, are still rare and require prior approval by the attorney general and sometimes the president.[81]

Back for More: Fuyi "Frank" Sun

In 2011, Mr. Sun contacted an aerospace company to procure export-controlled carbon fiber to ship to China.[1] Unfortunately for Sun, he had contacted a sting operation set up by the FBI to catch would-be procurement agents. During the undercover operation, FBI agents repeatedly asked Sun if he intended to apply for an export license, to which he indicated that he would. However, after failing to obtain a proper export license, Sun indicated that he intended to ship the carbon fiber to an intermediary country and then re-export the goods to China—all through an offshore company.

Although initial discussions failed because Sun felt the FBI might be monitoring his activity, it was not enough to deter him from returning to the fake aerospace company four years later in 2015 to set up additional deals. Eventually, Mr. Sun traveled to the United States in 2016 in order to meet with "representatives." Undercover agents eventually arrested Sun after he paid agents $25,000 in cash and explained how he would repackage and mislabel the items in order to transship through Australia on to China.

1 United States of America v. Fuyi Sun, aka "Frank," 1:16-CR-00404 Southern District of New York (April 13, 2016).

79 U.S. Department of Justice, Office of Legal Counsel, "Authority of the Federal Bureau of Investigation to Override International Law in Extraterritorial Enforcement Activities," June 21, 1989, p. 163.

80 U.S. Department of Justice, Office of Legal Counsel, p. 164.

81 The U.S. Supreme Court has ruled that prosecutors can still try a person who is arrested overseas and brought back to the United States without the consent of the country where he or she was arrested. See, U.S. Department of Justice, "United States Attorneys' Manual," secs. 9–15.610. These cases are most commonly associated with extraordinary rendition, like the case of Fawaz Younis—a Lebanese hijacker who was abducted overseas by the United States in 1987. Younis was tried in an American court and found guilty of committing terrorist acts against American citizens. He served thirty years in prison. For a summary of these cases, as well as other extraordinary renditions related to terrorism, see Tim Naftali, "The Perils of Extraordinary Rendition," *Slate Magazine*, June 30, 2005, http://www.slate.com/articles/news_and_politics/war_stories/2005/06/milan_snatch.html (accessed February 11, 2019).

Information awareness campaigns. In 2013, Congress established the Transnational Organized Crime Rewards (TOCR) program, which directs the Secretary of State to issue rewards for information on those involved in transnational crime, like human trafficking, money laundering, and dealing in arms and other illicit goods."[82] The TOCR program is primarily based on a similar program for narco-traffickers, the Narcotics Reward Program, which the Department of State established in 1986.[83]

Thus far, U.S. law enforcement authorities have used the TOCR program against only one WMD proliferator—Chinese national Li Fangwei (aka Karl Lee).[84] The State Department's reward for Lee's capture also coincided with the issuance of an FBI "Wanted" poster. He is listed in the Counter-intelligence section of the FBI's website alongside nine other individuals including spies, hackers, and intellectual property thieves. The U.S. State Department also placed a $5 million bounty for information leading to Lee's arrest as part of its Transnational Organized Crime Rewards Program.

While "Wanted" posters and rewards programs are not necessarily extra-territorial applications of U.S. domestic law, they are useful tools for raising awareness in foreign territories. Law enforcement agencies, like the FBI, have used "Wanted" posters since the 1920s— famously depicting gang-sters like "Pretty Boy" Floyd and John Dillinger, to Osama bin Laden. It is unknown, however, how effective these programs are for counterprolifer-ation. Karl Lee received little attention in the Chinese press after the U.S. imposed sanctions and issued its criminal indictment. Coupled with the Red Notice, however, such programs serve to not only raise awareness but limit Lee's travel. It is also possible that rewards programs and increased transparency compel Lee to alter his business operations in such a way as

82 "Narcotics Rewards Program," U.S. Department of State, https://www.state.gov/j/inl/narc/re-wards/index.htm (accessed August 30, 2018).

83 As of 2012, the Narcotics Reward Program paid out $71 million and had led to the arrest of several narco kingpins. Brooke M. Darby, "The State Department's Rewards Programs: Performance and Potential," (March 7, 2012), https://2009-2017.state.gov/j/inl/rls/rm/185410.htm (accessed Febru-ary 11, 2019).

84 "Transnational Organized Crime Rewards Program: Li Fangwei," U.S. Department of State, https://www.state.gov/j/inl/tocrewards/c62805.htm (accessed August 30, 2018).

to provide an opportunity for law enforcement to take action—perhaps by undermining trust within his organization.[85]

The Intersection of Law Enforcement and Regulation

The most common methods of disrupting proliferation network activities today exploit the structure of international financial systems. They range from targeted sanctions and banking regulations to the use of civil and criminal courts. In some cases, these tools allow enforcement agencies to gather critical intelligence to identify key network nodes and members, while other tools can disrupt the network directly by blocking access to the U.S. financial system or through seizures of proliferator assets.

The power behind these financial tools is derived mainly from the ability to leverage the strength and role of the U.S. dollar in the global financial system. In 2017, the U.S. dollar accounted for approximately 64 percent of the world's reserve currency. According to SWIFT—a Belgium-based company that facilitates a major share of secure financial messaging between international banks—approximately 40 percent of customer and institutional payments are conducted in U.S. dollars (based on value).[86] While this presents several opportunities for imposing legal jurisdiction around the world, it also poses significant challenges.

Section 311. As previously mentioned, Section 311 of the USA PATRIOT Act grants the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) the authority to declare a "foreign jurisdiction, financial institution, class of transactions, or type of account" to be a "primary money laundering concern." After the designation, FinCEN can require U.S. financial institutions and agencies to implement one or more of the "special measures," to include: maintaining certain detailed records, ob-

85 For discussions on the intersections between criminology and WMD proliferation, see Daniel Salisbury, "Why Do Entities Get Involved in Proliferation? Exploring the Criminology of Illicit WMD-Related Trade," *The Nonproliferation Review*, February 1, 2018, pp. 1–18; Arnold, "A Resilience Framework for Understanding Illicit Nuclear Procurement Networks."

86 "RMB Tracker," SWIFT, https://www.swift.com/our-solutions/compliance-and-shared-services/business-intelligence/renminbi/rmb-tracker/document-centre (accessed September 25, 2018).

Designation of Banco Delta Asia (BDA)

In September 2005, the United States designated Banco Delta Asia (BDA) under Section 311 of the PATRIOT Act. BDA was alleged to have been involved in North Korean money laundering and facilitating transactions relating to North Korean counterfeit currency and narcotics smuggling. At the time, the BDA designation was the first in a case related to WMD proliferation activities.[1]

As part of the designation, the United States declared Banco Delta Asia as a "bank of primary money laundering concern," and worked with Macanese authorities to freeze $25 million in North Korean assets. Although the amount seized was rather paltry compared to the sum of North Korea's illicit activities, the message sent shockwaves throughout the global financial system, compelling many international financial institutions to cut ties with the bank, fearing damage to reputation and losing access to the U.S. financial system. The United States later allowed the $25 million to be unfrozen and transferred out of BDA to a Russian bank and then to North Korea, as part of diplomatic efforts to curb North Korea's nuclear activities in June 2007.

1 Press release, "Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act" (U.S. Department of the Treasury, September 15, 2005), https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx (accessed February 11, 2019). Previous Section 311 designations were primarily related to terrorism or other types of transnational crime.

taining true beneficial ownership information, identifying correspondent customers, and the most serious, denying U.S. institutions from opening certain correspondent or pass-through accounts. The last special measure is the most severe because it denies foreign entity access to the U.S. financial system. Since 2001 there have been only eleven designations under Section 311.

FinCEN imposed its most recent Section 311 designation against China-based Bank of Dandong for wittingly acting as a gateway for North

Korea to evade international sanctions.[87] In 2016, several accounts at Bank of Dandong were used to facilitate millions of dollars of transactions on behalf of North Korean companies involved in the procurement of ballistic missile technology and other designated entities. The bank, for example, held several accounts for Korea Mining Development Corporation (KOMID), which was sanctioned by the United States and the UN for being a primary exporter of goods and technologies relating to ballistic missiles and conventional arms.[88] Under the FinCEN ruling, U.S. banks are prohibited from opening or maintaining correspondent accounts with Bank of Dandong.

Special Designations. Authorities granted to the Department of the Treasury's Office of Foreign Assets Control to blacklist entities from U.S. financial and commercial systems provide a further set of tools. These tools are based, in part or in whole, on either statutory authorities like the Iran Sanctions Act or executive actions, and implemented under Chapter V of the Code of Federal Regulations, which define the type and extent of prohibited financial and commercial transactions with persons or entities placed on the Specially Designated Nationals (SDN) list, as well as the civil penalties for violations. Since 2008, OFAC has imposed more than $4 billion in fines and penalties.

From an enforcement perspective, an SDN listing has two potent effects. The first is that designated entities are directly prohibited from accessing U.S. financial and commercial institutions, which can, in effect, directly disrupt procurement activities. In some cases, where the designee's assets are within U.S. jurisdiction, OFAC can order the assets to be blocked—i.e., frozen.[89] The second effect is more indirect. That is, the threat of civil penalties from OFAC or export violations will compel financial institutions and other businesses to enhance their compliance

87 "Imposition of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern," *Federal Registrar* 82, No. 215 (November 8, 2017).

88 KOMID was designated under Executive Orders 13382 and 13687 in July 2005, and UNSCR 1718 (2006) in April 2009.

89 Concerning prohibited transactions, there are generally two options for the financial institutions. If there is not an OFAC interest in blocking the transaction, the financial institution must reject the transaction. If there is a blocking order against any of the entities party to the underlying transaction, the bank must comply with the order (i.e., freeze the funds), and place the funds in an interest-bearing account until the party in question is no longer a Specially Designated National or entity. After assets are rejected or frozen, interested parties to the transaction do have the right to an administrative appeals process.

and risk programs to adhere to U.S. regulations, even if the company is not headquartered in the United States.

Apart from OFAC authorities, the U.S. Department of Commerce (DOC) has several administrative tools at its disposal to deny or restrict exports and re-exports under the Export Administration Regulations. For example, the DOC Bureau of Industry and Security maintains the denied persons list, which prohibits U.S. companies from exporting or re-exporting regulated goods to listed persons, as well as an entity list, which requires U.S. companies to first obtain a license before exporting or re-exporting any items listed within the Export Administration Regulations. These lesser-known tools can have the same or similar effects as an OFAC designation.

Secondary Sanctions. Another indirect tool with extraterritorial implications, which has gained in popularity over the last decade, has been the threat and use of secondary sanctions. Unlike the SDN list, which imposes targeted sanctions against those directly involved in WMD proliferation, secondary sanctions target non-U.S., third-party entities in foreign jurisdictions. Under the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA), for example, OFAC can impose sanctions against a foreign financial institution for conducting business with designated Iranian financial institutions—even if those transactions do not directly violate OFAC transaction regulations (that is, even if the transactions are not denominated in U.S. dollars and do not transit the U.S. financial system). Under CISADA, OFAC can impose several penalties, including prohibiting U.S. banks from opening and maintaining correspondent accounts—similar to the penalties under a Section 311 designation. Most recently, President Trump authorized secondary sanctions to be imposed against foreign financial institutions that "conducted or facilitated any significant transaction on behalf of any person whose property and interests in property are blocked" in connection with North Korea-related activities.[90]

90 "Executive Order 13810, Imposing Additional Sanctions With Respect to North Korea," September 25, 2017, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13810.pdf (accessed February 11, 2019).

ZTE Corp.

In March 2017, ZTE Corp. settled a civil liability action for several OFAC violations. Under the settlement, ZTE Corp. agreed to pay a fine of more than $100 million for 251 apparent violations of the Iranian Transactions and Sanctions Regulations (31 C.F.R. Part 560).[1] Between January 2010 and March 2016, ZTE Corp. exported and re-exported U.S.-origin goods to Iran using a network of third-party companies in order to conceal the transactions and illegal business with Iran. There was extensive evidence in internal company documents that senior officials of the company knew the transactions were contrary to sanctions rules and actively conspired to conceal them and lie to U.S. authorities. In addition to the penalty imposed by OFAC, ZTE Corp. also settled criminal penalties with the Department of Commerce and Department of Justice for $661 million and $430 million, respectively.[2]

The ZTE Corp. case is unique because most of the evidence required to support a legal action was located outside of U.S. jurisdiction. In order to compel ZTE Corp. to turn over documents requested by the Department of

1 Press release, "Zhongxing Telecommunications Equipment Corporation Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations," (U.S. Department of the Treasury, March 7, 2017).

2 Karen Freifeld and Sijia Jiang, "China's ZTE Pleads Guilty, Settles U.S. Sanctions Case for Nearly $900 Million," *Reuters*, March 8, 2017, https://www.reuters.com/article/us-usa-china-zte/chinas-zte-to-pay-over-800-million-to-settle-with-u-s-over-iran-sales-source-idUSKBN16E1X1 (accessed February 11, 2019).

The United States has threatened secondary sanctions to achieve its political aims far more often than it has enforced secondary sanctions. In the case of Iran, secondary sanctions—under CISADA—were imposed against only two foreign financial institutions—Bank of Kunlun, which is a small Chinese bank, and Iraqi Elaf Bank.[91] Both were cited for knowingly facilitating significant transactions on behalf of sanctioned Iranian entities. Kunlun, for example, provided payment services totaling more than $100 million for Bank Tejarat—an Iranian bank directly involved in financing

91 Press release, "Treasury Sanctions Kunlun Bank in China and Elaf Bank in Iraq for Business with Designated Iranian Banks," (U.S. Department of the Treasury, July 31, 2012), https://www.treasury.gov/press-center/press-releases/Pages/tg1661.aspx (accessed February 11, 2019).

Commerce, the Bureau of Industry and Security (BIS) issued a "temporary general license," meaning if ZTE Corp. failed to comply, BIS would merely let the temporary license expire, in which case the company would be included on the BIS entity list—effectively being shut out of U.S. markets. In April 2018, the Commerce Department found ZTE Corp. to be in breach of the agreement, thereby imposing a seven-year export denial, which restricts all U.S. companies from conducting business with the Chinese telecommunications giant and prevents the company from doing business within the United States.[3] The action effectively forced the telecom giant to halt its global operations.[4]

Interestingly, the "snap-back" of the export ban was not due to export violations, but instead due to "a false or misleading statement" that ZTE Corp. produced regarding compliance with "employee disciplinary measures." In July 2018, President Trump intervened amid growing tensions between China and the United States over looming tariffs. Trump lifted the ban against ZTE Corp., imposed a $1 billion penalty, and required ZTE Corp. to restructure some of its upper management.[5]

3 Steve Stecklow, Karen Freifeld, and Sijia Jiang, "U.S. Ban on Sales to China's ZTE Opens Fresh Front as Tensions Escalate," *Reuters*, April 17, 2018, https://www.reuters.com/article/us-china-zte/exclusive-u-s-bans-american-companies-from-selling-to-chinas-zte-idUSKBN1HN1P1 (accessed February 11, 2019).

4 Edward White, "ZTE Shares Jump after Washington Lifts Ban on US Purchases," *Financial Times*, July 16, 2018, https://www.ft.com/content/df2c19ce-8894-11e8-bf9e-8771d5404543 (accessed February 11, 2019).

5 "US Lifts Order against China's ZTE," *BBC News*, July 13, 2018, https://www.bbc.com/news/business-44825878 (accessed February 11, 2019).

Iran's nuclear and ballistic missile activities, which was added to the OFAC SDN list in January 2012.[92]

Asset Forfeitures and Blockings. Another tool deployed by the United States to take direct action against overseas proliferators is the use of asset forfeiture procedures within domestic civil courts. The U.S. criminal money laundering statutes provide for both civil and criminal asset forfeiture for violations.[93] To be guilty of a money laundering violation the defendant

92 Press release, "Treasury Designates Major Iranian State-Owned Bank," (U.S. Department of the Treasury, January 23, 2012).

93 See, Section 317, *The USA PATRIOT Act*, 2001.

must have committed some underlying (i.e., predicate offense).[94] Because IEEPA violations are a predicate offense for money laundering, U.S. prosecutors can use domestic civil courts to target proliferator assets.

Unlike criminal asset forfeitures, civil forfeiture cases are conducted administratively *in rem*—meaning, against the defendant's property. Moreover, the systems of due process for civil forfeiture cases are entirely different from those of a criminal nature and generally favor the prosecution, especially when the defendant is unable to appear in court. Whereas a criminal forfeiture requires a conviction where the evidentiary burden is on the prosecutor to prove guilt beyond a reasonable doubt, a civil case merely requires an evidentiary standard of the "preponderance of evidence." In other words, the prosecutors must demonstrate that the transactions in question are more likely than not to be connected to an underlying crime (i.e., an IEEPA or other specified unlawful activity). This "51 percent" standard is significantly lower than proof beyond a reasonable doubt.

The USA PATRIOT Act significantly enhanced civil asset forfeiture authorities by empowering prosecutors to target illicit funds held overseas, outside of U.S. jurisdictions. Section 319 of the Act amends U.S. forfeiture statutes to include interbank (i.e., correspondent) accounts. Explicitly, the code states that:

> *…if funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a covered financial institution…the funds shall be deemed to have been deposited into the interbank account in the United States, and any restraining order, seizure warrant, or arrest warrant in rem regarding the funds may be served on the covered financial institution, and funds in the interbank account, up to the value of the funds deposited into the account at the foreign bank, may be restrained, seized, or arrested.*

In other words, prosecutors can indirectly seize proliferator assets held overseas by targeting the foreign bank's accounts within the United States. To date, however, U.S. prosecutors have been somewhat reluctant to fully leverage these authorities to target North Korean or Iranian illicit proceeds.

94 In general, money laundering is the concealment of proceeds from illicit activity.

Targeting North Korea's Offshore Illicit Financing Networks

The most recent cases of civil asset forfeiture targeted North Korea's networks of intermediaries and financiers that allow the regime to evade international sanctions and access the global financial system. In September 2016, U.S. prosecutors brought a civil case against Dandong Hongxiang Industrial Development (DHID) in the District of New Jersey for violating IEEPA and conspiracy to commit IEEPA violations.

According to the criminal complaint, Ma Xiaohong and her top executives established more than twenty-two front companies around the world to help North Korea's Kwangson Banking Corp., which was sanctioned in 2009 for its role in financing dual-use procurement, maintain access to global banking networks.[1] Using shell companies registered in secrecy jurisdictions like Seychelles and the British Virgin Island, DHID acted as a payment processor for U.S. dollar-denominated transactions on behalf of North Korean banks.

Under the civil forfeiture action, U.S. prosecutors seized $74 million from 25 separate bank accounts held by DHID at several Chinese banks.[2] These Chinese banks ranged in size from large national institutions to small regional banks. However, importantly, each had correspondent relationships with U.S. institutions, where prosecutors can serve the seizure warrants.

1 United States of America v. Dandong Hongxiang Industrial Development Co. Ltd, U.S. District Court (n.d.).

2 These included China Merchants Bank, Shanghai Pudong Development Bank, Bank of Communications Co. of China, Bank of Dandong, China Construction Bank, Guangdong Development Bank, Industrial and Commercial Bank of China, Bank of Dalian, Bank of Jinzhou, Hua Xia Bank, and China Minsheng Banking Corporation.

For one, such actions may damage U.S. relations with the host country. There have been only four such instances to date; the first case was against Karl Lee and the most recent cases involved North Korean networks in China.[95]

95 For a full discussion of these recent cases, see Aaron Arnold, "Solving the Jurisdictional Conundrum: How US Enforcement Agencies Target Overseas Illicit Procurement Networks Using Civil Courts," *The Nonproliferation Review*, September 24, 2018, pp. 1–22.

Similar to the ability to seize assets held in correspondent accounts, prosecutors have also successfully employed peremptory or "damming" warrants to seize transactions that have not yet occurred but may. Peremptory warrants place a "metaphorical dam" at a financial institution in order to catch incoming transactions that are connected to an underlying unlawful activity. As soon as the transaction arrives, the banks freeze the funds. Recently, U.S. prosecutors successfully obtained a damming warrant to seize transactions related to North Korea sanctions evasion. In May 2017, the U.S. District Court for the District of Columbia issued a 14-day warrant, which required the financial institution to monitor for and freeze any transactions by Dandong Zhicheng Metallic Co. Ltd. According to court records, Dandong Zhicheng was using U.S. correspondent banks to facilitate coal-related trade on behalf of sanctioned North Korean entities.[96]

Unlike the previously mentioned civil forfeiture case, where the transactions had already occurred, the damming warrant puts into place a net to catch future transactions. This, of course, can be a complicated process that requires significant coordination among law enforcement and banking institutions given the sheer number of transactions that U.S. institutions handle each day. Moreover, it is not always clear to law enforcement and financial institutions when or where the transaction will occur, which is one reason why prosecutors rarely use damming warrants.

Active Engagement with Financial Institutions. Although not necessarily a disruption tool, U.S. officials have not shied away from conducting direct negotiations and talks with foreign financial institutions and regulators to close accounts associated with proliferation networks. Dubbed the "whisper campaign," former Treasury Department Under Secretary Stuart Levy would routinely meet with the heads and CEOs of foreign banks to discuss how Iran used the global financial system to facilitate illicit procurement and evade international sanctions.[97] In one such instance, Levy provided evidence to the executive staff of a German bank showing how the Iranian Revolutionary Guard Corps (IRGC), which was sanctioned under UNSCR 1929 (2010), was using front and shell companies to evade sanctions and

96 United States of America v. Dandong Zhicheng Metallic Material Co., LTD, District Court (United States, 2017).

97 Juan Carlos Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: Public Affairs, 2013), p. 300.

procure nuclear proliferation-sensitive equipment and technology. According to Juan Zarate, a senior Bush administration official, the "whisper campaign" was effective—the German bank, among others, began shuttering accounts linked to Iranian entities.[98]

Implications of Expanding Law Enforcement Counterproliferation Extraterritoriality

As noted throughout this report, U.S. counterproliferation law enforcement efforts have increasingly leveraged extraterritorial tools in order to contend with the transnational nature of illicit WMD procurement, weak international trade controls, and the lack of multilateral legal frameworks. Many of these law enforcement activities take advantage of legal and regulatory reforms made following the September 11, 2001 terrorist attacks. While flexing extraterritorial law enforcement capabilities may address jurisdiction problems in counterproliferation efforts, they also create several legal and political challenges.

From a legal perspective, most U.S. counterproliferation criminal and regulatory activities rely on IEEPA authorities, which can be problematic for fostering international cooperation. What constitutes an IEEPA violation, for example, is at the discretion of the president, which creates a subjective legal framework that is unique to U.S. foreign policy interests and often politically driven, or at least perceived in that way. Also, international law enforcement cooperative arrangements generally adhere to a principle of dual criminality. Foreign governments are far more likely to cooperate with U.S. enforcement and extradition requests when the criminal act is also a specified crime in the foreign jurisdiction. Since an IEEPA criminal violation is dependent on corresponding executive orders, which can vary significantly depending on the type of security threat, it is quite unlikely

98 Zarate, p. 301. Swiss bank UBS and Credit Suisse announced in 2006 that they would end their business ties with Iran. See "UBS Cancels Business with Iran," *MarketWatch*, January 22, 2006, https://www.marketwatch.com/story/ubs-cancels-business-with-iran (accessed February 11, 2019). After Trump withdrew the United States from the JCPOA in May 2018, his administration set about to convince EU leaders and banks to cut off Iran from its banking system. Since then, U.S. allies have strongly criticized Trump for his reversal on the JCPOA and the use of financial and economic sanctions in a manner not consistent with the intent of the JCPOA.

that a foreign jurisdiction would have a similar criminal statute to satisfy dual-criminality requirements or cooperate based on a temporary legal authorization. Thus, without a common legal ground for overseas counter-proliferation activities, U.S. law enforcement is left to use extraterritorial (i.e., non-cooperative) authorities, which in turn reduces incentives for international cooperation.

Unilateral law enforcement activities in non-cooperative jurisdictions may also undermine broader multilateral nonproliferation efforts—like, fostering global political commitments to implementing UNSCR 1540 obligations. China, for example, has consistently opposed U.S. unilateral actions against its citizens. After the designation and asset forfeitures against Karl Lee in 2014, a spokesman for China's Foreign Ministry criticized the United States for its actions and suggested it would harm future joint nonproliferation efforts between the two countries.[99] In August 2017, when the Trump administration imposed sanctions against a number of Chinese and Russian individuals and companies responsible for facilitating North Korea's access to the international financial system, Chinese officials strongly criticized U.S. "long-arm jurisdiction" and promised to oppose any further unilateral actions taken over Chinese entities and individuals.[100] In the case of ZTE Corp., China warned that it was "prepared to take action to protect the interests of Chinese firms…"[101]

While China has been the target of most U.S. proliferation-related extraterritorial enforcement actions in recent years, European allies have become increasingly alarmed over continued expansions of extraterritoriality and emerging threats against E.U. political and economic interests. In August 2018, the Trump administration re-imposed sanctions against Iran after unilaterally withdrawing from the JCPOA in April. In addition to prohib-

99 Rick Gladstone, "China: Criticism of U.S. Move on Iran," *The New York Times*, April 30, 2014, https://www.nytimes.com/2014/05/01/world/asia/china-criticism-of-us-move-on-iran.html (accessed February 11, 2019).

100 Carol Morello and Peter Whoriskey, "U.S. Hits Chinese and Russian Companies, Individuals with Sanctions for Doing Business with North Korea," *The Washington Post*, August 22, 2017, https://www.washingtonpost.com/world/national-security/us-sanctions-chinese-and-russian-companies-and-individuals-for-conducting-business-with-north-korea/2017/08/22/78992312-8743-11e7-961d-2f373b3977ee_story.html (accessed February 11, 2019).

101 Stecklow, Freifeld, and Jiang, "U.S. Ban on Sales to China's ZTE Opens Fresh Front as Tensions Escalate"; Sijia Jiang, "U.S. Ban on Sales to ZTE Triggers Patriotic Rhetoric in China," *Reuters*, April 19, 2018, https://www.reuters.com/article/us-usa-china-zte/chinas-zte-removed-chief-compliance-officer-before-u-s-sanction-source-idUSKBN1HQ0S2 (accessed February 11, 2019).

iting U.S. individuals and companies from conducting business and trade with Iran, the sanctions also target foreign entities—i.e., secondary sanctions. In a May 2018 speech, President Trump quipped that "Any nation that helps Iran in its quest for nuclear weapons could also be strongly sanctioned by the United States."[102] Later that month, the Treasury Department advised all non-U.S., non-Iranian entities "…to wind down their activities with or involving Iran that will become sanctionable at the end of the applicable wind-down period."[103]

European leaders strongly condemned the U.S. unilateral actions and committed to "…mitigating the impact of U.S. sanctions on European businesses and taking steps to maintain the growth of trade and economic relations between the EU and Iran that began when sanctions were lifted."[104] In terms of action, the European Commission amended a 1996 regulation, known as the Blocking Statute, meant to insulate European companies against American secondary sanctions against Cuba, Libya, and Iran. In principle, the Blocking Statute shields against U.S. extraterritoriality by providing a legal indemnification for EU companies and individuals. That is, the statute provides a legal basis for EU entities to *not* comply with U.S. measures by nullifying the effect, within the EU, of any foreign decision based on extraterritorial legislation (e.g., U.S. secondary sanctions).[105]

Whether or not the Blocking Statute will be an effective bulwark to U.S. extraterritoriality remains to be seen. For one, the statute provides several types of exemptions for companies that may suffer financial harm by complying with the statute. It is also increasingly apparent that many large EU companies would rather forgo business opportunities in Iran than risk potential fines or restrictions from the United States—a decidedly larger

102 "Read the Full Transcript of Trump's Speech on the Iran Nuclear Deal," *The New York Times*, May 8, 2018, https://www.nytimes.com/2018/05/08/us/politics/trump-speech-iran-deal.html (accessed February 11, 2019).

103 The Trump administration provided 90-day and 180-day wind-down periods for companies that have business relationships with Iran.

104 Press release, "European Commission Acts to Protect the Interests of EU Companies Investing in Iran as Part of the EU's Continued Commitment to the Joint Comprehensive Plan of Action," (European Commission, May 18, 2018), http://europa.eu/rapid/press-release_IP-18-3861_en.htm (accessed February 11, 2019).

105 "Guidance Note: Questions and Answers: Adoption of Update of the Blocking Statute," Official Journal of the European Union, August 7, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOC_2018_277_I_0003&from=EN (accessed February 11, 2019).

market.[106] Several large European firms have signaled they will close their business ties with Iran. In November 2018, SWIFT relented to American pressure by restoring U.S. sanctions on Iran and booted most Iranian banks from its financial messaging service—a significant blow to EU efforts to keep the Iran nuclear deal intact.[107]

More importantly, though, the Blocking Statute demonstrates an increased frustration with U.S. extraterritorial actions. It is entirely possible that the political fallout from the U.S. withdrawal from the JCPOA and subsequent reimposition of sanctions will have negative consequences on broader counterproliferation efforts. For one, states may work to insulate themselves against U.S. extraterritoriality further. This, in turn, could have negative repercussions for joint-counterproliferation law enforcement and intelligence efforts, including information sharing and extradition requests. Also, states may view the U.S. unilateral withdrawal from the JCPOA and subsequent extraterritorial application of domestic law as a willingness to "go it alone" rather than uphold traditional international norms, which could affect states' decisions to fully implement their obligations under UNSCR 1540.

This section has provided an overview of the expanding toolset that the U.S. government has deployed in its efforts to counter WMD proliferation networks and more broadly conduct export control enforcement overseas. While these extraterritorial tools have provided unique opportunities to disrupt overseas illicit procurement networks, they have also raised new questions and challenges. The next section provides a set of recommendations to address these challenges and concerns.

106 See, for example, The Wisconsin Project on Nuclear Arms Control, "How Companies Around the World Are Reversing Course on Iran Business," Iran Watch, August 7, 2018, https://www.iranwatch.org/our-publications/policy-briefs/how-companies-around-world-are-reversing-course-iran-business (accessed February 11, 2019).

107 Michael Peel, "Swift to Comply with US Sanctions on Iran in Blow to EU," *Financial Times*, November 5, 2018, https://www.ft.com/content/8f16f8aa-e104-11e8-8e70-5e22a430c1ad (accessed February 11, 2019); Michael Peel, "US Rejects Europe's Hopes of Relief from Iran Sanctions," *Financial Times*, July 15, 2018, https://www.ft.com/content/6a16440a-8837-11e8-bf9e-8771d5404543 (accessed February 11, 2019).

Section 3: Recommendations and Conclusions

In this report, we detailed U.S. extraterritorial law enforcement approaches to countering WMD-related illicit trade, the legal and political challenges posed by operations beyond U.S. jurisdiction, and the broader implications for global counterproliferation efforts. While extraterritorial enforcement demonstrates a strong commitment to controlling the spread of WMD-related goods and technology, such measures can also erode trust and may undermine efforts to ensure consistent implementation of norms and obligations, such as those articulated in UNSCR 1540. Additionally, unmitigated extraterritorial enforcement has the potential to undermine broader international security and economic objectives. Chinese officials, for example, viewed recent law enforcement actions against a Huawei executive as a strong-arm tactic by the Trump administration. In all likelihood, however, the arrest was part an ill-timed, ongoing investigation. Nonetheless, the arrest threatened to undermine ongoing U.S.-China trade negotiations.

Thus, it is important that the United States work toward finding a balance between extraterritorial law enforcement activities and committing to a multilateral approach to global nonproliferation objectives—especially for implementing global strategic trade controls. The U.S. government should place particular effort on mitigating the potential unintended consequences associated with extraterritorial enforcement.

Enhancing Domestic Integration and Collaboration

As previously discussed, U.S. counterproliferation law enforcement activities are spread over several agencies with few points of integration. This can lead to overlapping objectives, investigations, and operations, which can frustrate or undermine overseas enforcement activities. In order to more effectively coordinate extraterritorial enforcement activities, the Trump administration should appoint a director of counterproliferation law enforcement to serve on the National Security Council (NSC) staff

under the Senior Director for Counterproliferation Strategy. The director would be responsible for coordinating a comprehensive assessment of U.S. counterproliferation enforcement activities, as well as developing a national strategy that integrates broader U.S. and international nonproliferation objectives.

The assessment should consist of a bottom-up examination of all U.S. law enforcement agencies that engage in counterproliferation-related activities, their authorities, and their impact on national counterproliferation goals and objectives. This assessment should explore ways to reduce redundancy and overlap by increasing information-sharing and coordination, and also explore ways to maximize the efficacy of inter-agency organizations, like the Export Enforcement Coordination Center (E2C2), and reduce incentives to silo counterproliferation investigations and operations within specific agencies. This includes not only funding liaison activities between agencies but ensuring proper agency representation in overseas legal attaché offices, as well as with international police organizations, like INTERPOL. The director should work closely with the White House Office of Management and Budget to determine appropriate funding levels and necessary resources consistent with the strategy's goals and objectives.

The NSC director for counterproliferation law enforcement should also consider gaps in agency capacity and capability regarding knowledge, training, human resources, legal authorities, and technology. For example, different case management and information technology systems can present challenges concerning inter-agency coordination and collaboration. Information about the tools and techniques available to investigators to target and disrupt overseas procurement networks, for example, can vary significantly by agency and office. This includes both the type of information available to investigators, as well as an understanding of the applicable legal constructs (e.g., criminal or civil). Specific training available to law enforcement and intelligence officials on overseas disruption tools is scarce and with no centralized forum. For example, some training courses are only available to law enforcement, while others are only available to members of the intelligence community. Others are not well advertised or held infrequently. This is especially evident when it comes to employing the range of novel financial disruption tools, such as civil asset forfeiture.

Finally, Congress, with input from the national czar and heads of relevant agencies, should explore updating criminal and civil law to reflect broader consistency with international norms. In other words, the United States should seek to reduce reliance on the criminal penalties found under the International Emergency Economic Powers Act. Recently, Congress passed the Export Control Reform Act (2018), which codifies certain aspects of the Export Administration Act, in addition to giving new law enforcement authorities to offices within the U.S. Department of Commerce. While the legislation is a significant step forward in comprehensive export control reform, it does very little toward delineating roles and responsibilities and ensuring a consistent approach to law enforcement activities for countering WMD-related illicit trade. A stand-alone criminal statute will help U.S. law enforcement agencies establish dual-criminality with foreign partners, thereby helping to reduce the need to "go it alone" in many cases.

Maintaining both Capability and Legitimacy

Extraterritorial enforcement is not an unlimited resource. It comes with political costs that could ultimately undermine or reduce the efficacy or capability to conduct future extraterritorial actions. Over the last decade, policymakers have increasingly viewed sanctions and other extraterritorial actions as cost-effective, low-risk, and reproducible policy instruments; they appear to have largely ignored these tools' potential hazards.[108] These hazards are most significant when extraterritorial enforcement actions are carried out without broad international consensus on the larger objectives. Consequently, states have become increasingly alarmed at the expansion of U.S. extraterritoriality and what some see as politicization of the international financial system. The Obama administration's "whisper campaign" among European banks to isolate Iran was effective because the United States made clear that pressuring Iran was part of a broader engagement strategy to achieve a diplomatic resolution to the Iranian nuclear crisis. By

108 Aaron Arnold, "The True Costs of Financial Sanctions," *Survival*, Vol. 58, No. 3 (May 3, 2016), pp. 77–100; Elizabeth Rosenberg et al., "The New Tools of Economic Warfare: Effects and Effectiveness of Contemporary U.S. Financial Sanctions" (Washington, D.C.: Center for a New American Security, April 2016).

contrast, the Trump administration's threats to impose secondary sanctions may force companies to withdraw their business from Iran in the short term, but the U.S. withdrawal from the JCPOA is nearly universally seen as illegitimate, even by its closest European allies. Over time, both countries and companies may take steps to reduce their vulnerability to U.S. actions they see as capricious, which could weaken future counterproliferation enforcement, the dominance of the U.S. financial system and the role of the U.S. dollar as the international reserve currency, and U.S. relations with both allies and countries such as China and Russia.

Although the reach of U.S. extraterritorial enforcement is significant, countries are not without options to resist. In recent years, several states have moved to insulate themselves against exposure to U.S. sanctions. China and Russia, for example, have each developed alternative payment systems in order to avoid dollar-dominated systems. Global companies are also seeking to limit their exposure to U.S. sanctions by exiting high-risk jurisdictions that may incur additional scrutiny by the US—a process dubbed "de-risking."[109]

Despite legal protections guaranteed by the European Council, EU companies are exiting Iranian markets out of fear of U.S. unilateral sanctions. On one hand, these trends illustrate the power and influence of U.S. extraterritorial policies. On the other hand, these trends also expose potential downsides and the risks of overuse. U.S. enforcement actions are prompting adaptation that may ultimately undermine law enforcement's ability to identify and disrupt overseas illicit networks. For example, as banks de-risk from foreign jurisdictions, useful financial intelligence goes unreported. From a law enforcement and intelligence perspective, this creates blind spots in foreign jurisdictions where transparency is needed the most. Therefore, it is imperative that policymakers begin to calibrate U.S. extraterritorial law enforcement and regulatory actions in order to avoid overuse.

109 Randall Mikkelsen, "Bankers Say 'derisking' Underway amid Sanctions Crackdown; That's the Point, U.S. Regulator Says," Financial Regulatory Forum, *Reuters*, October 3, 2014, http://blogs.reuters.com/financial-regulatory-forum/2014/10/03/bankers-say-derisking-underway-amid-sanctions-crackdown-thats-the-point-u-s-regulator-says (accessed February 11, 2019).

To do so, the administration must think strategically about the relationship between U.S. sanctions policies and extraterritorial law enforcement actions and their effects on broader nonproliferation objectives and commitments. This effort will require additional cooperation between law enforcement and diplomatic agencies in such a way as to maintain a dollar-dominated global financial system. The United States must monitor the ways states are adapting to U.S. extraterritoriality and how that adaptation could affect future U.S. capabilities. Moreover, this will require a much more comprehensive understanding of how extraterritorial enforcement actions and sanctions policies affect national-level nonproliferation objectives. Next, the administration should take care to minimize the use of extraterritorial tools that impinge on the national sovereignty of others.

Instead, preference should be given to options that make use of official legal procedures while adhering to international rules and norms, in the service of nonproliferation objectives that enjoy consensus international support (or near-consensus support). Multilateral cooperation should remain a cornerstone of U.S. counterproliferation efforts. As previously discussed, outdated legal agreements and differences in national legislation can frustrate law enforcement-to-law enforcement cooperation. Thus, the Department of State, in concert with the Departments of Treasury and Justice, should work to update its mutual legal assistance treaties (MLATs) to incorporate legal definitions and standards consistent with contemporary interpretations of jurisdiction concerning export controls and nonproliferation objectives. Moreover, the U.S. must continue to reaffirm its commitments to multilateral approaches to supply-side controls, including by increasing outreach, capacity-building, and technical training to developing countries.[110]

Relatedly, and perhaps somewhat ambitiously considering current political tensions, the U.S. should not shy away from engaging in discussions with Chinese authorities about export control implementation, enforcement, and cooperation. While China now has extensive export control legislation, its enforcement mechanisms continue to lack appropriate resources and directives. While this presents an obvious opportunity for coordination, U.S.

110 See, Matthew Bunn et al., *Preventing Black Market Trade in Nuclear Technology* (New York: Cambridge University Press, 2018), pp. 350–352.

law enforcement cooperation with China—historically—has been a mixed bag. On issues relating to national security and illicit procurement, China has been less than forthcoming. As previously mentioned, China continues to refuse to take action against Karl Lee, even as suspicions now mount that Lee's activities continue unabated. There have been successful liaison efforts—especially insofar as addressing transnational criminal activity like narcotics trafficking and counterfeiting.[111] Strengthening law enforcement cooperation can be done as part of ongoing trade negotiations, as well as through track-two efforts with Chinese organizations, like the China Arms Control and Disarmament Association. Although it is unlikely that the United States and China will come to an agreement or statement of principles, it is feasible to come to a mutual understanding of each's goals and objectives.[112]

Finally, the administration should take concerted steps to avoid entangling national political objectives with international rules-based systems. Section 311 designations, for example, can undermine international commitments to rules-based systems if applied indiscriminately. International bankers became concerned with the Bush administration's decision to freeze North Korean assets at Banco Delta Asia under the auspices of money laundering violations, only to lift the freeze once North Korea agreed to rejoin the six-party nuclear negotiations.

Increasing Financial Transparency

In general, law enforcement activities have moved little beyond treating the symptoms of illicit procurement, trying to punish proliferation actors as

111 In 2005, Chinese authorities provided substantial evidence and testimony to support a U.S. investigation and prosecution of an American living in Shanghai who ran a counterfeit DVD enterprise. Although many thought this case represented a thaw in law enforcement liaison between the two countries after decades of non-cooperation, subsequent liaison efforts have been less than fruitful.

112 Consider, for example, the December 2018 U.S. extradition request to Canada for Chinese citizen Meng Wanzhou. Ms. Meng is a top executive at Huawei—a major Chinese telecommunications company—and wanted by the U.S. authorities for violating sanctions against Iran. The timing of the extradition request has coincided with tense trade negotiations between President Trump and China's president Xi Jinping. While all accounts suggest this is a case of bureaucratic dysfunction and lousy timing, Chinese authorities have called foul—suggesting that the U.S. is using its extraterritoriality to strong-arm China during trade negotiations. Anna Fifield, David J. Lynch, and Ellen Nakashima, "China's Judgment on Huawei Case: Anger, Patriotism and iPhone Boycotts," *The Washington Post*, December 11, 2018, https://www.washingtonpost.com/world/asia_pacific/chinas-judgment-on-huawei-case-anger-patriotism-and-iphone-boycotts/2018/12/11/5861371c-fa54-11e8-8642-c9718a256cbd_story.html (accessed February 11, 2019).

they come up on the radar screen. But so far, enforcement actions against overseas procurement agents seem have had little deterrent effect. A key reason is a persistence of enabling institutions, like financial secrecy jurisdictions—i.e., tax havens.[113] If deterrence is a preferred consequence of law enforcement, then overseas networks must have some awareness of and sensitivity to risk.

The United States should pursue new policies that target enabling institutions—global institutions that allow procurement agents to hide overseas, free from the risk of getting caught. One of the key strategies for U.S. enforcement activities should be to increase the cost-benefit thresholds for overseas procurement agents—i.e., increasing the risk of getting caught. From a criminological perspective, the certainty of punishment, rather than the magnitude of punishment, usually has a more significant deterrent effect.[114] This fact, however, does not necessarily mean increasing extraterritorial enforcement actions will produce the desired result.

The cases reviewed in this report illustrate how networks illicitly procure WMD-related goods and technologies by exploiting legal and regulatory transnational gaps in financial, supply chain, and logistics systems worldwide—creating jurisdictional hurdles for U.S. law enforcement efforts. Interestingly, illicit networks have generally exploited the same legal and regulatory gaps for decades. A now declassified report by the Central Intelligence Agency, for example, shows that in the early 1980s, networks trafficking in gray-market nuclear technologies exploited financial secrecy jurisdictions, made extensive use of front companies, falsified end-user certificates, made alterations on export applications, and relied on transshipment through third countries with weak export control laws.[115] Take, for example, the recent case against Dandong Hongxiang Industrial Devel-

113 Although there is no formal definition of a secrecy jurisdiction, they are typically defined by their lack of transparency, with financial rules and regulations that allow participants to hide huge sums of money with no questions asked and little knowledge of who really owns the accounts. Some common features include tax secrecy rules that prohibit cooperation with law enforcement and regulatory authorities, hidden beneficial ownership information of registered companies, and weak anti-money laundering rules. In fact, in some jurisdictions, like Panama, it is against the law to turn over banking records to certain legal authorities. This makes secrecy jurisdictions ideal venues to stash ill-gotten gains or hide illicit procurement operations

114 For a discussion that links criminology to illicit procurement, see Salisbury, "Why Do Entities Get Involved in Proliferation? Exploring the Criminology of Illicit WMD-Related Trade."

115 "The Gray Market in Nuclear Materials: A Growing Proliferation Danger" (Central Intelligence Agency, July 1984), p. 4, https://www.cia.gov/library/readingroom/document/cia-rdp85t00287r000600940003-2 (accessed February 11, 2019).

opment Co., which was a China-based network that helped a sanctioned North Korean bank maintain access to the global financial system—including access to U.S. banks. The laundering scheme used no less than 22 shell companies established in secrecy jurisdictions like the British Virgin Islands, the Seychelles, and Hong Kong.[116]

U.S. approaches to addressing the problem of secrecy jurisdictions have been relatively slow, but legislation introduced in 2017 by Congresswoman Carolyn Maloney, entitled the *Corporate Transparency Act*, would go a long way to addressing corporate secrecy in the United States and would signal a U.S. commitment to corporate transparency. In addition to refreshing its corporate secrecy laws and regulations, the United States should also consider targeted financial sanctions against foreign secrecy jurisdictions that are known to habitually facilitate sanctions evaders and proliferation financiers. The United Kingdom, for example, recently took concerted steps to enhance corporate transparency by requiring its overseas territories, including the Cayman Islands, the British Virgin Islands, and Bermuda, to make public the owners of all registered companies.[117]

Conclusion

There is little doubt that supply-side controls will remain a staple within the U.S. nonproliferation arsenal for years to come. As global trade and commerce in dual-use goods and technologies continues to grow, the issue of jurisdiction will remain a prominent challenge for counterproliferation activities. This report has highlighted how networks of middlemen and intermediaries involved in the illicit procurement of weapons of mass destruction-related goods and technologies often operate outside of the United States, which presents several legal and political challenges for U.S. enforcement activities.

116 David Thompson, "In China's Shadow: Exposing North Korean Overseas Networks" (C4ADS, August 2016).

117 Madison Marriage and Henry Mance, "Caymans, Bermuda and BVI Face New Corporate Transparency Laws," *Financial Times*, May 1, 2018, https://www.ft.com/content/8cc0e314-4d47-11e8-97e4-13afc22d86d4 (accessed February 11, 2019).

As others have rightly pointed out, successful global supply-side controls require a multilateral approach that brings to bear diplomatic, regulatory, law enforcement, and intelligence resources.[118] To that end, however, it is important also to consider how extraterritorial enforcement may negatively (or disproportionately) affect such efforts, as well as undermine global nonproliferation norms. While the long arm of U.S. law enforcement can address several of these jurisdictional shortcomings, the use of extraterritorial enforcement mechanisms must not become perceived as an easy substitute or alternative for upholding broader nonproliferation commitments.

118 Bunn et al., *Preventing Black Market Trade in Nuclear Technology*.

Project on Managing the Atom
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/mta

Printed in the United States of America