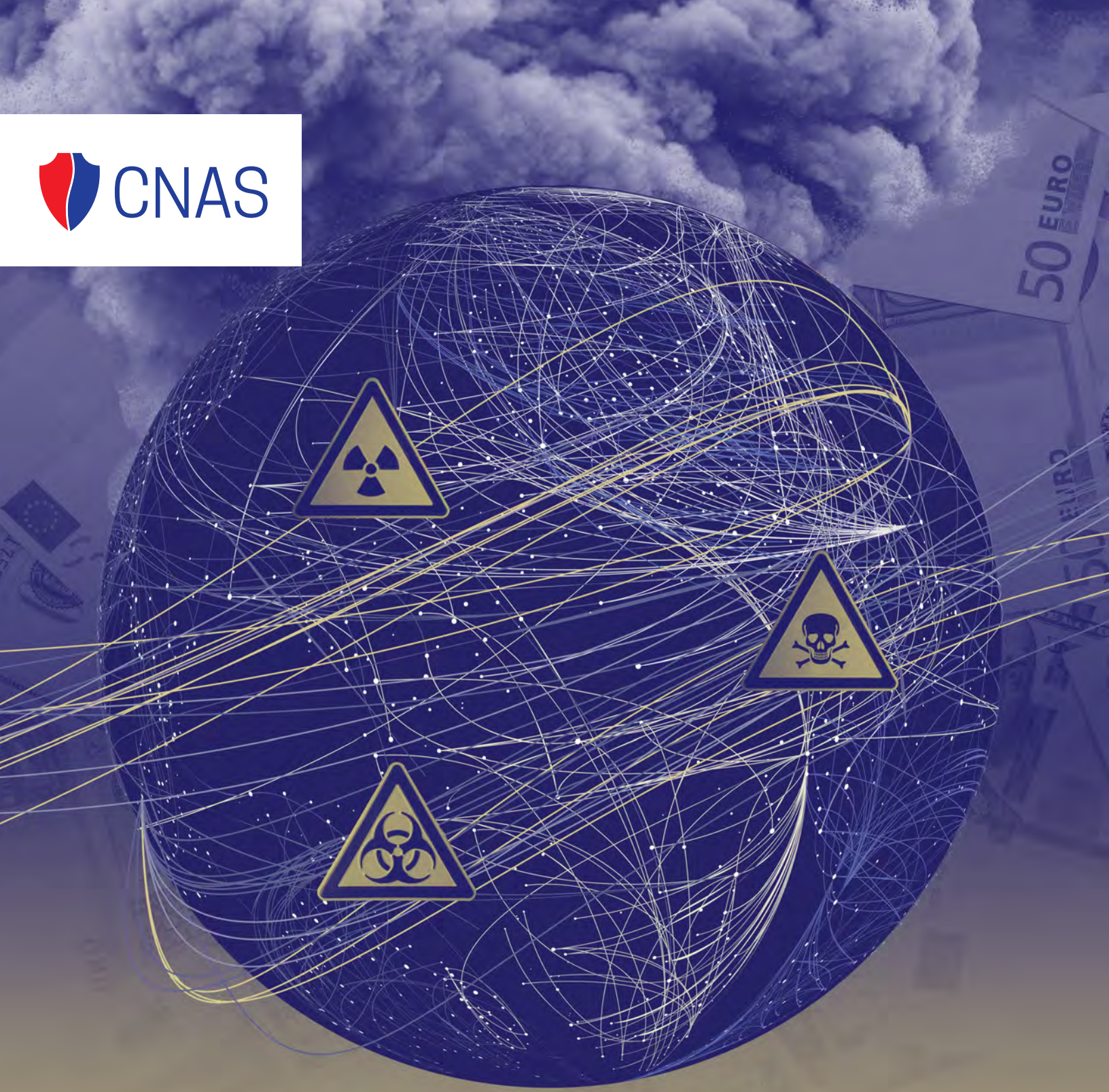


DECEMBER 2018

Financial Networks of Mass Destruction

Elizabeth Rosenberg, Neil Bhatiya, Claire Groden, and Ashley Feng

About the Authors

ELIZABETH ROSENBERG is a Senior Fellow and Director of the Energy, Economics, and Security Program at CNAS. Previously, she served as a Senior Advisor at the U.S. Department of the Treasury on international illicit finance issues, helping senior officials develop financial sanctions and formulate anti–money laundering and counterterrorist financing policy.

NEIL BHATIYA is the Research Associate for the Energy, Economics, and Security Program at CNAS. His work focuses on the geopolitics of energy, climate change, and tools of economic statecraft. Prior to joining CNAS, he was the Climate and Diplomacy Fellow at the Center for Climate and Security. He was previously a Fellow at the Century Foundation.

CLAIRE GRODEN is a JD candidate at NYU School of Law and former Program Associate at the Center on Law and Security at the law school. Previously she worked as a reporter at *Fortune* and *The New Republic* magazines. She holds a bachelor's degree from Dartmouth College in government and Asian studies, and a master's of law (Chinese studies) from Peking University, where she was a Yenching Scholar.

ASHLEY FENG is a Research Assistant in the Energy, Economics, and Security Program at CNAS, focusing on East Asia and China. Previously she was a Research Associate for China Studies at the Council on Foreign Relations, where she researched U.S. policy toward China and Chinese foreign policy.

Acknowledgements

The authors would like to thank Loren DeJonge Schulman for her review of this report. They also thank Zachary Goldman, Sue Eckert, Jonathan Brewer, and Frederick Reynolds for their valuable ideas and feedback during the drafting of the report. Finally, they would like to acknowledge Melody Cook, Tristan Campos, and Maura McCarthy for their assistance with the production of this report.

This report was made possible by the generous funding of the John D. and Catherine T. MacArthur Foundation.

About the Energy, Economics & Security Program

The Energy, Economics, and Security Program analyzes the changing global energy and economic landscape and its national security implications. From the shifting geopolitics of energy to tools of economic statecraft, such as trade policy and sanctions, to security concerns tied to a changing natural environment, the program develops strategies to help policymakers understand, anticipate, and respond. The program draws from the diverse expertise and backgrounds of its team and leverages other CNAS experts' strengths in regional knowledge, defense, and foreign policy to inform conversations in the nexus of energy markets, industry, and U.S. national security and economic policy.

Cover Photo
Images: Getty Images; Design: Melody Cook/CNAS

FINANCIAL NETWORKS OF MASS DESTRUCTION

Executive Summary

Key Takeaways

- The lack of effective and universal financial controls to prevent weapons of mass destruction (WMD) proliferation is a gaping security vulnerability for the international community.
- Illicit actors, including those acting on behalf of countries such as Iran and North Korea, have exploited, are exploiting, and will continue to exploit these vulnerabilities.
- The United States has unique power and responsibility to combine domestic legislative and regulatory reforms with international leadership in order to strengthen the countering proliferation finance regime. Doing so will require overcoming significant political will obstacles.

The international community has long prioritized reducing the risk of weapons of mass destruction proliferation, whether from state actors such as North Korea and Iran, or from non-state actors, particularly criminals and transnational terrorist networks. Despite this concern, however, there remains a significant blind spot: the efforts to prevent the financing of WMD proliferation are only in their infancy. The legal framework to prevent the financing of proliferation is weak, and implementation across the world is spotty. These weaknesses derive from one overwhelming fact: The international community has not prioritized financial controls to fight proliferation. Very few countries have demonstrated the political will to put further emphasis on this threat to international peace and security.

The role of the United States is essential in building a stronger regime to counter proliferation finance. As the world's largest economy, with a sophisticated financial sector, well-resourced law enforcement and intelligence capabilities, and the ability to restrict access to the U.S. dollar, the United States has a great deal of leverage in helping those countries that wish to do more, and in compelling laggard countries to focus more intensively on the issue.

This is a crucial national security concern for the United States, even though to date it has not been approached as such. These networks are quite sophisticated at evading detection and know how to exploit weak regulations and enforcement in jurisdictions around the world. North Korea and Iran in particular have operated (and North Korea continues to operate) egregious, publicly documented, sophisticated global networks of trusted agents. These networks have contributed significantly to what had been an active uranium-enrichment program (in the case of Iran), and a substantial nuclear weapons capability (in the case of North Korea). These states are creative and diligent in developing new ways to continually disguise their activities, pioneering new technology and networks to sustain themselves and grow. The United States has prioritized dealing with North Korea and Iran as high-level security threats, but the proliferation finance aspect of that strategy has been woefully underdeveloped.

Stepping up action to combat the financing of proliferation will take legal change at home, including financial transparency measures and new methodologies to facilitate information sharing between banks and between banks and national authorities. It will also require intensive leadership in international forums such as the Financial Action Task Force (FATF) and at the United Nations (U.N.) to elevate due diligence and compliance around preventing the financing of proliferation. This will include revising FATF's recommendations to incorporate more proactive risk-based measures so that countries are judged on more than just compliance with screening against a list of proliferators subject to sanctions. The latter should focus on strengthening the work of the United Nations Security Council

The weaknesses in the regime derive from one overwhelming fact: The international community has not prioritized financial controls to fight proliferation.

Resolution (UNSCR) 1540 nonproliferation committee, improving the guidance that FATF provides on proliferation finance, and encouraging dozens of countries to improve their legal frameworks and dedicate the required level of attention and resourcing to fulfill their international obligations.

The risk of inadequately responding to the risk of proliferation finance is stark. The use of a weapon of mass destruction by a malign state actor or a non-state actor, especially a nuclear one, would be a generation-defining catastrophe. In the aftermath, the international community would ask what went wrong. What such a retrospective would discover is that such capabilities may have been facilitated through ordinary commercial channels. The response to such a discovery may have broad macroeconomic consequences. Avoiding that disaster, and the growth of threats emanating from WMD stockpiles in the hands of rogue actors, is the goal of this report.

Strong measures to counter proliferation finance must be a key piece of a holistic approach to national security policy.

This report explores the weaknesses of the current countering proliferation finance regime. Using case studies, it highlights how a lack of political will allows proliferation networks to obtain goods and move money in violation of international controls. It offers a survey of the current legal framework for approaching countering proliferation finance. This framework provides some important tools to U.S. and international authorities, but is alarmingly weak in many areas. The report then discusses how even a solid legal framework may flounder because of fundamental problems with political will at the national and international levels. It then offers recommendations for the United States and its international partners to build a much stronger countering proliferation finance regime. The report is designed to help security and foreign policy leaders understand the gravity of the issue and the necessity of elevating countering proliferation finance work in broader nonproliferation activities and analysis of transnational threats, especially North Korea and Iran policy. It argues that strong measures to counter proliferation finance must be a key piece of a holistic approach to national security policy, and it outlines a roadmap for how to get there.

Introduction

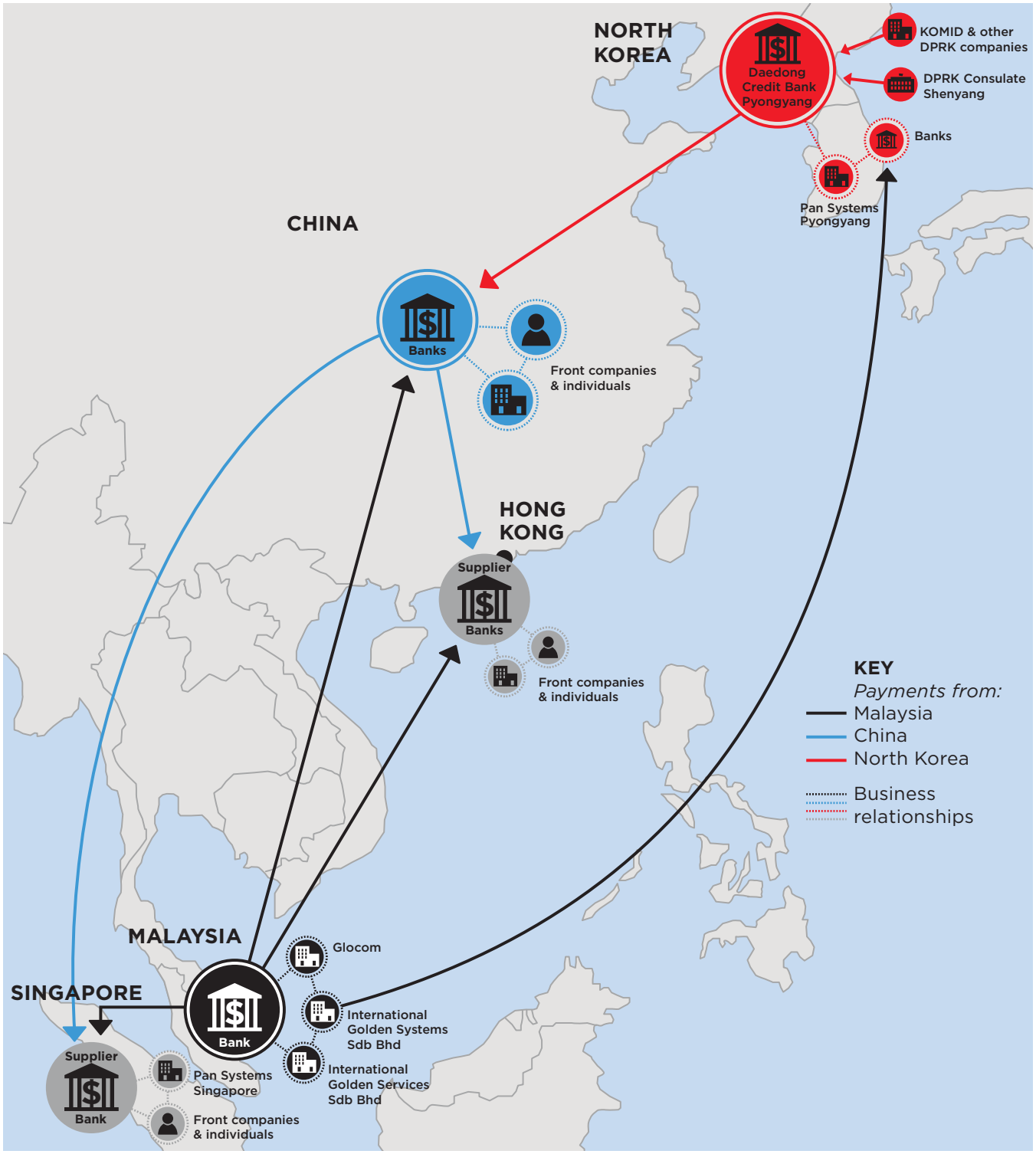
In December 2012, the Republic of Korea salvaged the debris of an Unha-3 rocket, which the Democratic People's Republic of Korea (DPRK) had used to launch a satellite into orbit. The launch was particularly alarming given the potential for the rocket to carry a nuclear warhead. Pyongyang's sophisticated nuclear program has for decades been a prominent national security concern for the United States, its allies South Korea and Japan, North Korea's ally China, and the wider international community.

After an exhaustive review, nonproliferation and illicit finance experts from the United Nations Panel of Experts on North Korea discovered the origins of many of the components the North Koreans used to build the rocket. Despite U.N. sanctions and the international consensus that Pyongyang obtaining sophisticated missile capabilities is a critical threat to international peace and security, the Unha-3 contained materials that had been manufactured in China, the former Soviet Union, the United Kingdom, Switzerland, and the United States, almost certainly transacting in currencies from major Western economies.[1]

As concerning as it was that North Korea was able to procure materials from advanced democracies and the world's leaders on nonproliferation policy, just as alarming is that many of the components were off-the-shelf items that were not included on export control lists designed to prevent goods from falling into the hands of proliferating states. The fact that North Korea was able to obtain commercial goods with such ease is a stark

The wreckage of North Korea's Unha-3 sits at the 2nd Fleet Command's naval base on December 14, 2012. The U.N. Panel of Experts concluded that materials in Unha-3 had been manufactured in China, the former Soviet Union, the United Kingdom, Switzerland, and the United States. (Yeong-Wook/DongA Daily/Getty Images)

Figure 1: North Korea's Procurement Networks[130]



A simplified illustration of North Korea's sophisticated procurement networks, based in multiple countries. In this case, Pan Systems Pyongyang and its front companies carry out financial activity in multiple jurisdictions, which benefits, among others, the Korea Mining and Development Trading Corporation (KOMID), which is widely considered to be North Korea's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. Pan Systems Pyongyang's involvement in Middle East business is referenced without details (not shown).

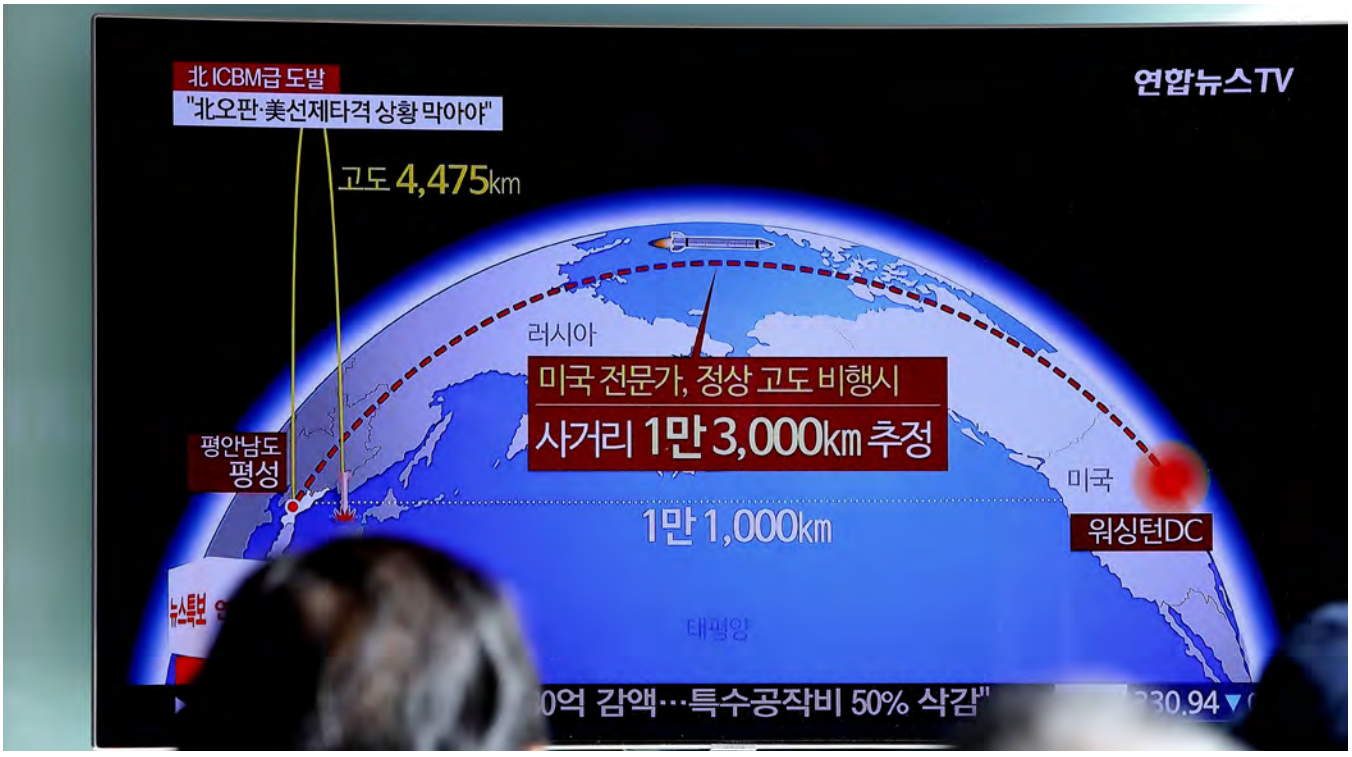
demonstration of the extent to which its proliferation networks have penetrated the international financial system. The ability of these networks to use shell companies to exploit globalized supply chains, penetrate financial networks to obtain goods not on export control lists, and obtain know-how threaten North Korea's neighbors and the world. This underscores the challenges facing financial institutions in trying to discover illicit activity.

The construction of the Unha-3 with internationally sourced components, procured using international financial channels, is but one example of what the financing of weapons of mass destruction proliferation looks like in practice. Figure 1 offers an illustrative example of how complex these networks are. North Korea, as well as Iran – especially before the implementation of the Joint Comprehensive Plan of Action (JCPOA) – Syria, India, and Pakistan, have all been at the forefront of global security concerns about how illicit and covert weapons of mass destruction programs are financed and supplied with materials.

What Is Proliferation Finance?

In contrast to the nuclear weapons programs of advanced industrial states, many U.S. adversaries do not have the indigenous research, development, and deployment capacity to constitute weapons of mass destruction programs entirely on their own. As a result, they have to seek financial resources, goods, and know-how elsewhere, including from reputable industrial firms throughout the world, especially from the United States and Europe. The illicit networks that procure these goods and the revenue to sustain illicit WMD programs represent a serious national security threat: financing of proliferation is a critical backbone, the essential money trail, that enables rogue states, and non-state actors, to threaten peace and security.[2] These networks dupe and abuse public and private sector institutions alike, and cultivate complicit insiders. The stakes for this dirty money movement are high, and the response to date has been woefully and alarmingly lacking.

It is possible to detect and track the financing of proliferation. By going outside their own national borders to find support for illicit weapons programs, proliferating states leave themselves open to discovery by the international community. If moving money in exchange for goods is essential to building a weapons of mass destruction program, then it becomes possible for financial regulators, law enforcement, and intelligence agencies to track and disrupt it, and, where possible, to apprehend



North Korea fired an intercontinental ballistic missile for the first time in four months in November 2017. Components of many North Korean rockets are procured from companies in advanced democracies, many of whom are considered world leaders on nonproliferation policies. (Chung Sung-Jun/Getty Images)

members of the proliferation networks. Shutting down the money trail for proliferators can be a powerful and effective tool to check the devastating threat posed by rogue states with nuclear weapons. Ultimately, cracking down on the financing of illicit activities is an effective way to stop the illicit activity itself.

This is easier said than done. The issue facing the international community is that these networks are quite sophisticated at evading detection and know how to exploit weak enforcement in jurisdictions around the world. North Korea and Iran, in particular, have operated (and, in the case of North Korea, continues to operate) egregious, publicly documented, sophisticated global networks of trusted agents. These networks have contributed significantly to what had been an active uranium-enrichment program (in the case of Iran), and a substantial nuclear weapons capability (in the case of North Korea). These states are creative and diligent in developing new ways to continually disguise their activities, pioneering new technology and networks to sustain themselves and grow.[3]

In the wake of the U.S. withdrawal from the Iran nuclear deal, known as the Joint Comprehensive Plan of Action (JCPOA), it is possible that Iran may try to restart a nuclear-enrichment program, including potential steps to weaponization. Prior to the JCPOA, Iranian-affiliated actors had been implicated in a number of proliferation finance cases. In one case, Iran procured components for its nuclear and ballistic missile program through a complex structure of payments channeled through banks in France, the United Arab Emirates, and Turkey to obtain materials from a Spanish manufacturer. The Iranian company in question was able to get around a denial of an export license by Spanish authorities for electrical discharge machines by using two different countries of transshipment.[4] Examples like this are important because they emphasize the truly global reach of these networks.

North Korea's evasion of international controls stands in stark contrast to its purported interest in assuring the international community that it is committed to normalization.

In the case of North Korea, despite the ongoing diplomatic process between the Kim Jong-un regime and the Trump administration, it is far from clear that Pyongyang is on a path to denuclearization. In fact, attempts to procure proliferation-related goods appear to continue unabated, as evidenced by recent United Nations Panel of Experts reports. North Korea's evasion of international controls stands in stark contrast to its purported interest in assuring the international community that it is committed to normalization of relations.[5]

Members of President Trump's cabinet and closest advisors have articulated concerns that Iran may try to restart its nuclear-enrichment program. (Chip Somodevilla/Getty Images)

In the face of this persistent, even potentially expanding threat, the international community is willfully blind to the notion that policy and financial leaders, ideally together, can do much more to prevent the growth of illicit nuclear weapons. Foreign policy, security, and nonproliferation experts around the world unquestioningly accept a doctrine that extraordinary financial pressure and controls have tried and failed to constrain rogue proliferators. This assumption is wrong – the controls and pressure have never been, and still are not, as comprehensive as they should be. The potential cost of failing to fix this weakness is stark: a confrontation with a nuclear-armed state or terrorist group able to build an arsenal with the help of reputable Western companies would be a catastrophic global governance failure.

The Role for the United States

The United States is well placed to correct this misperception and make a meaningful difference to check the global nuclear threat. Indeed, because the dollar is the global currency of choice for trade, investment, and as a reserve currency, and because the U.S. financial sector is the largest globally, the role of the United States to halt the financing of proliferation is vital. The current administration deserves credit for attempting to address this situation, but must do much more to focus maximum effort on constraining rogue countries' ability to pursue

an illicit weapons capability. This includes specific enforcement actions domestically, such as strengthening rules around financial transparency, extending safe harbor provisions for banks working creatively on finding proliferation finance typologies internally, and increasing resources for national law enforcement, and regulatory and intelligence agencies. It also means

Because the U.S. financial sector is the largest globally, the role of the United States to halt the financing of proliferation is vital.

making countering proliferation finance the first priority for its presidency of FATF, the global standard setter for financial crimes regulation.[6] This will furthermore strengthen the control regime to the point that it can prevent proliferation threats from other countries and non-state actors much sooner. Financial network analysis is a key part of threat detection and evaluation for that effort, and the United States and the international community must use levers within the financial system to identify and deter the proliferation threat. The United States and certain jurisdictions in Western Europe, for example the United Kingdom, have built very powerful legal and regulatory powers to investigate, disrupt, and prosecute a wide variety of financial crimes risks, including money laundering and corruption. This is the base for attacking dirty money.

What is needed now is political will to fill in the gaps for the countering proliferation finance regime. The historic current lack of will stands in bewildering contrast to the clear and intensive concern that international policymakers have about the threats of weapons of mass destruction, particularly the use of nuclear weapons. The United States in particular has gone to great lengths to counter proliferation threats. The Trump administration has spent an enormous amount of political and diplomatic capital ensuring that North Korea and Iran cannot threaten their neighbors with nuclear weapons. With this base and the leverage that it has created, the U.S. administration must put in place the legal regime and policy guidance to better prevent the financing of nuclear-weapons proliferation.

Accomplishing this will take legal change at home, including with financial transparency measures and new methodologies to facilitate information sharing between banks and between banks and national authorities. It will also require intensive leadership in international forums such as FATF and at the United Nations to elevate due diligence and compliance around preventing the financing of proliferation, including revising FATF's recommendations to incorporate more proactive risk-based measures so that countries are judged on more than just compliance with sanctions. The latter should focus on strengthening the work of the United Nations Security Council Resolution 1540 nonproliferation committee, improving the guidance that FATF provides on proliferation finance, and encouraging dozens of countries to improve their legal frameworks and dedicate the required level of attention and resourcing to fulfill their international obligations.

Other jurisdictions look to the United States as an example because of the centrality of the U.S. dollar to international commerce. The size of its financial sector means that U.S. regulations directly and indirectly affect firms worldwide. U.S. intelligence and law enforcement capabilities are also unparalleled in finding and stopping these activities. The unique scale of these capabilities also gives the United States diplomatic heft in bilateral interactions with partners and allies facing risk because of proliferation financing, as well as in multilateral institutions where these issues are addressed, for example the U.N. and FATF.

The legal and administrative solutions are not hard to articulate. They include fixing gaps in national legislation, financial regulations, export controls, and other oversight mechanisms for global commerce. The truly difficult work for the United States will be urging, or compelling, the political will to fight the financing of proliferation, and reducing institutional resistance to sharing information with the private sector. Even though all U.N. member states are obligated under Chapter VII

In November 2017, the United Nations Security Council held an emergency meeting concerning North Korea's nuclear ambitions after that nation test-fired an advanced intercontinental ballistic missile days earlier. (Drew Angerer/Getty Images)

authority of the United Nations Charter to comply with Security Council resolutions aimed at combating WMD proliferation and its financing – and indeed many profess the will to do so – many sophisticated and well-resourced states do not.

An open secret of an enormous array of countries is that they are unwilling, or see themselves as unable, to sacrifice the economic advantages of looking the other way. They may even knowingly facilitate proliferation. For some countries, allowing North Korea to penetrate their financial system is lucrative, or affords political and diplomatic dividends, as discussed in the case studies in this report. These examples, which are notorious and in some cases date back decades, underscore the complex political calculations that serve as roadblocks for necessary action.

The Peril of Willful Blindness and Failure to Prioritize

The weaknesses of the regime to counter proliferation finance contrasts markedly with how the international community handles efforts to counter terrorist financing. Two decades ago, the U.S. Treasury Department and relevant agencies in the U.S. intelligence community had tried to track al Qaeda's finances following the 1998 embassy bombings in Kenya and Tanzania, though it was not a high-priority effort, either within the United States government or internationally. Richard Clarke, President Clinton's top terrorism advisor, cited U.S. intelligence officials who downplayed targeting financing by saying that terrorist groups like al Qaeda "didn't need a lot of money."[7] However, over time the effort to counter terrorist financing was buttressed by a strong international framework: the United Nations had adopted a counterterrorist financing convention in 1999, and it was aided by specific U.N. Security Council resolutions, such as 1267 (1999). Enormous international political will to implement a holistic regime to counter the financing of terrorism coalesced after the disaster of 9/11. Global policy leaders realized after these attacks that following the money trails could be a blueprint to mapping the network and understanding – perhaps even anticipating – its moves.

In order to ultimately track Osama bin Laden to his Pakistani safe house, the U.S. intelligence community was able to use knowledge about the channels he used to circulate information and money. Bin Laden relied on couriers to convey messages and financial resources between him and his network of agents elsewhere in Pakistan, Afghanistan, and around the world. The documents seized in the raid on his headquarters offered extensive insight into al Qaeda's operations and plans.[8] During the past decade and a half, individual states and the international community built a sophisticated regime for countering the terrorist financing threat.[9]

But now the threat is evolving. Terrorist plots are overwhelmingly homegrown in the West (73 percent of attacks in Europe and North America from 2014 to 2017 were homegrown), and there is an uptick in incidents in Europe, with attacks increasing 7 percent from 2016 to 2017.[10] As a result, the regulation and practices to track and impede terrorist financing are becoming increasingly sophisticated and nuanced, taking a strong system and adapting it to present-day circumstances in a way that should serve as a model for other examples of countering threat finance.[11]

The risk now is that the international community will wake up to proliferation finance only after a similar paradigm-shifting event. The stakes are high and, based on expanding proliferation threats, it is certainly possible that we will learn a bitter lesson about the significance of countering proliferation finance efforts only after a major nuclear event has occurred. One of the gravest challenges for security leaders today is to avoid repeating an underestimation of the contemporary terrorist threat. In this case, this means realizing too late how blind and complicit we have been in allowing banks, businesses, and national governments to help grow rogue nuclear weapons arsenals.

This report offers a survey of the current legal framework for countering proliferation finance. As it now stands, this framework provides some important tools to U.S. and international authorities but is weak in many areas. The report then discusses how even a solid legal design may be inadequate because of fundamental problems with political will at the national and international levels. It then offers recommendations for the United States and its international partners to build a much stronger countering proliferation finance regime. This report is designed to help security and foreign policy leaders understand the gravity of the issue and the necessity of elevating work in countering proliferation finance to broader nonproliferation activities and analysis of transnational threats, especially with regard to policy for North Korea and Iran. Arguing that strong measures to counter proliferation finance must be key in a holistic approach to national security policy, this report outlines a roadmap for how to get there.

The Current Legal Framework: Strong Initial Steps with Many Gaps to Fill

Frameworks to combat proliferation rely on three interlinked layers: international legal obligations put into place by the United Nations; the soft law framework, exemplified by FATF's recommendations; and domestic law. All three of these layers impact the risk management practices of global banks. In 1946, the United Nations General Assembly's very first resolution created a commission "to investigate the problems raised by the discovery of atomic energy." More than 70 years later, countering the proliferation of weapons of mass destruction remains a foundational goal of the international community.

The Security Council Committee established pursuant to Resolution 1540 (2004) (1540 Committee) monitors the implementation of Resolution 1540 (2004), which obligates states to have and enforce measures against the proliferation of nuclear, chemical, and biological weapons by non-state actors. The Security Council Committee established pursuant to resolution 1718 Committee (2006) (1718 Committee) is specific to North Korea's proliferation threat. It designates individuals and entities engaged in or providing support for North Korea's WMD programs, and individuals or entities who act at their behest. The 1718 Committee also monitors other restrictions on North Korean economic activity, such as its procurement and sale of energy resources, among other measures. But one tool in the counter-proliferation arsenal – countering the financing of proliferation – remains poorly understood and figures minimally in U.N. nonproliferation obligations, even as the international community increasingly seeks to use financial methods to rein in the nuclear programs of Iran and North Korea.

U.S. Secretary of State Mike Pompeo chairs a United Nations Security Council meeting on North Korea. Since the beginning of the Trump administration, the U.N. Security Council has passed four resolutions establishing tighter economic restrictions on North Korea. (Spencer Platt/Getty Images)

The global push to specifically counter the financing of proliferation had a promising start in 2004, when the U.N. Security Council passed Resolution 1540, a remarkably sweeping resolution that demanded member states enact comprehensive frameworks to prevent WMD proliferation and its financing by non-state actors. Unlike nearly all Security Council resolutions, which react to specific conflicts, this resolution sought to counter proliferation broadly, and it required member states to overhaul their sovereign laws in specific ways in order to do so.

Unfortunately, however, the drafters of Resolution 1540 (2004) concentrated primarily on controls on goods and materials, and it contains only two narrow references to financing: under operational paragraph 2, all member states are required to implement legislation to prohibit financing of manufacture, acquisition, possession, development, transport, transfer, or use of WMD, and their means of delivery, by non-state actors. Under operational paragraph 3(d), all states are required to implement controls on financing the export or transshipment of WMD and their means of delivery, and related materials.

Under operational paragraph 12 of a subsequent resolution, 2325 (2016), the 1540 Committee is required to continue to intensify efforts to promote full implementation of Resolution 1540 (2004). In particular, the need for more attention to proliferation finance measures, *inter alia*, is noted. Resolution 2325 (2016) is the first use of the term "proliferation financing" in a Security Council resolution, but, except insofar as Resolution 2325 (2016) is a successor resolution, the term is not defined.

Resolution 1540 (2004) on nonproliferation was unanimously approved by the Security Council in the aftermath of the discovery of Abdul Qadeer (A. Q.) Khan's WMD proliferation network (thus the primary focus of the resolution is on non-state actors: the businessmen, fixers, commercial traders, factory owners, etc., whom the network comprised, and also the terrorists seeking the capabilities). As of October 2018, 12 U.N. member states had yet to submit a report on implementation, as called for by the Security Council.[12]

A relevant U.N. resolution for comparing approaches to targeting the financing of a transnational security threat, Resolution 1373, was enacted weeks after the 9/11 attacks to establish similarly comprehensive frameworks to counter terrorism and its financing. The notably rapid and thorough implementation of Resolution 1373 was as

In 2002, when border tensions were running high in South Asia, Pakistan test-fired a medium-range surface-to-surface missile. Pakistan has been at the forefront of global security concerns related to proliferation finance. (Handout/Getty Images)

unprecedented as the resolution itself, with all members submitting a first report, as called for by the council within a year and a half of the resolution's adoption.[13] Member states widely criminalized acts of terrorism in their domestic laws, and the financing of terrorism was added to FATF's portfolio the same year it was enacted.[14]

The U.N. does require member states to counter state-led proliferation, with attention to financial channels, through a series of Iran- and North Korea–related resolutions. Targeted financial sanctions are at the core of such measures, but the provisions extend more widely to include activity-based sanctions, requirements for vigilance, and other prohibitions, for example on dealings with North Korean financial institutions and on financial services that could contribute to North Korea's WMD programs.

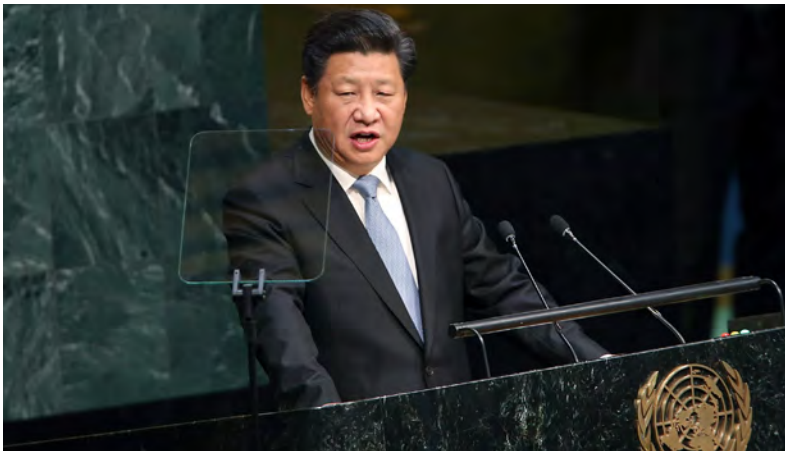
Gaps in International Focus and Implementation

U.N. member states have not pursued implementation of Resolution 1540 with the same level of political dedication as counterterrorism financing obligations. Some of these gaps are for legal reasons, which are addressed is this section. Due to a complex set of political, diplomatic, and economic circumstances, which are unique to each member state, violations of international obligations, many of which are brazen and well-documented, are allowed to occur.

Legally, one of the major challenges to states wishing to formulate domestic countering proliferation finance measures is that, unlike countering terrorist financing, working against proliferation finance measures is not linked to a specific international convention.[15] Additionally, member states are not prioritizing the clarification of how much effort 1540 requires to fight the financing of proliferation by states, as opposed to non-state actors. This misses the point that state proliferators such as North Korea, Iran, Syria, Pakistan, India, and others usually rely at least in part on overseas procurement networks made up of non-state actors – the primary target of Resolution 1540 (2004).

But significant problems also surround implementation of country-specific U.N. sanctions. As testified by numerous U.N. Panel of Export reports, as well as by independent analysts using open-source information, the vast majority of U.N. member states do not heed the requirements of U.N. sanctions and provide financial resources to the regime in North Korea, or they allow companies operating in their jurisdictions to facilitate transactions in violation of sanctions. Many sub-Saharan African states have had North Korean military personnel on their soil to provide training in exchange for cash that can be used by the regime to sustain and expand its proliferation programs, to cite one prominent set of violations.[16]

In other instances, some U.N. member states, including members of the Security Council, block more aggressive action for political or diplomatic reasons. Russia and China weakened U.N. Security Resolution 2375 (2017),



Chinese President Xi Jinping delivers remarks at the United Nations General Assembly. Behind the scenes at the United Nations, China, along with Russia, weakened U.N. Security Resolution 2375, a nonproliferation resolution targeting North Korea. (Lintao Zhang/Getty Images)

The lack of transparency in the shipping industry provides support to the illicit networks looking to evade U.N. sanctions. To date it has been difficult to build an international coalition to interdict ships bound for North Korean ports because of international legal concerns. (Spencer Platt/Getty Images)

a nonproliferation resolution targeting North Korea, from its original draft that would have blacklisted Kim Jong-un, removed exceptions for all transshipments of Russia coal, and completely banned the hiring and payment of North Korean laborers abroad.[17] Similar to China, Russia also fears a collapse of the North Korean regime, which would result in a sudden influx of refugees to both China and Russia. A collapse could also result in possible conflict on the Korean Peninsula, as different powers try to seize control of North Korea's nuclear weapons.

To date, it has been very difficult to build an international coalition to interdict shipping bound for North Korean ports because of concerns that international law does not allow the forcible boarding of ships in international waters. Indeed, the ability of warships to legally board merchant vessels is quite limited: "A warship may only stop a merchant vessel if there is reasonable ground to believe (a) that the ship is engaged in piracy; (b) that the ship is engaged in the slave trade; or (c) that [though] flying a foreign flag or refusing to show its flag the ship is, in reality, of the same nationality as the warship."[18]

As the next section, "The Roadblocks Political Inaction and Inadequate Rules," will demonstrate, such activities are not solely a function of weaknesses around the legal regime, but rather have to do with much more fundamental questions of political will.

Gaps at the Financial Action Task Force

The United Nations is not the only multilateral institution that is struggling, or stumbling, with a response to proliferation finance. While proliferation financing was added to FATF's portfolio in 2008, differing member opinions about the role financial institutions could or should play in detecting financing of proliferation ensured that the effort remained a relatively low priority element of FATF's work. FATF's current standards, guidance, and ongoing attention, for example, are not nearly as comprehensive for proliferation finance as they are for countering terrorist financing or anti–money laundering. This is true even while the proliferation risk is recognized by FATF's members, and indeed the international community, as a prominent security threat on par with these other challenges. The FATF recommendations that emphasize the importance of a risk-based approach for anti–money laundering and countering terrorist financing measures do not extend the principle to proliferation finance. Specifically, FATF's one

recommendation solely related to proliferation finance, Recommendation 7, is quite limited in what it requires of FATF member states:

> Countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. These resolutions require countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.[19]

As FATF's own non-binding guidance on proliferation finance makes clear, however, targeted financial sanctions alone are an incomplete strategy to really counter proliferation networks. Most sophisticated actors know how to structure their activities to avoid the scrutiny of sanctions screening:

> However, the [sanctions] screening would not be sufficient on its own, as targeted financial sanctions are also applicable to persons/entities acting on behalf of or at the direction of designated persons/entities. This adds additional complexities for public and private sector entities in identifying and detecting the persons, entities, and transactions related to proliferation financing.[20]

The latest version from FATF expands on 2013 guidance related to non-targeted financial sanctions elements of the requirements of U.N. sanctions resolutions. Unfortunately, it says little about the financial requirements of UNSCR 1540, the fundamental building block of the U.N. framework to combat proliferation. This is a significant gap that FATF should address quickly. The effort to do this needs to be led, or at least strongly encouraged, by the United States, which is in a unique position to do so while it holds the FATF presidency.

Rick McDonell was the executive secretary of the Financial Action Task Force between 2007 and 2015, during which time FATF released a major typologies report on proliferation financing. FATF is the global standard setter for financial crimes regulation. (Aurelien Meunier/Getty Images)

Besides comprehensive reviews by the 1540 Committee, there are few tools that precisely measure the degree to which states have implemented proliferation financing measures. In 2016, a comprehensive review on the status of implementation of Resolution 1540 (2004) shows that few states have dedicated proliferation financing legislation in place.[21] However, in comparison with previous reviews, the 2016 report noted significant progress between 2008 and 2016, as described in Table 1. While the numbers of measures to prohibit and enforce the prohibition of financing of proliferation activities and measures on the financing of illicit WMD-related transactions had increased, most states had not addressed the need to prohibit the financing of means of delivery, especially for nuclear weapons.

The comprehensive review also highlighted that most states rely on counterterrorism financing measures to address problems with proliferation financing. Although there was an improvement in measures on the financing of illicit WMD-related trade transactions, this was largely due to increased and improved legislation on counterterrorism financing, money laundering, and the establishment of financial intelligence units.

TABLE 1
Financial Measures to Control WMD Proliferation under Resolution 1540 (2004)

		NUMBER OF STATES		
		2008	2011	2016
LEGISLATION IN PLACE (obligations under operative paragraph 2)	**NUCLEAR WEAPONS**	66	124	158
	CHEMICAL WEAPONS	71	129	166
	BIOLOGICAL WEAPONS	64	122	161
ENFORCEMENT MEASURES IN PLACE (obligations under operative paragraph 2)	**NUCLEAR WEAPONS**	78	119	155
	CHEMICAL WEAPONS	87	121	161
	BIOLOGICAL WEAPONS	75	114	156
MEASURES TO CONTROL FINANCING OF ILLICIT WMD-RELATED TRADE (obligations under Operative Paragraph 3(c) and Operative Paragraph 3(d))	**NUCLEAR WEAPONS**	-	33	109
	CHEMICAL WEAPONS	-	37	110
	BIOLOGICAL WEAPONS	-	35	109

Source: United Nations Security Council, Letter from the Chair of the Security Council Committee Established Pursuant to Resolution 1540 (2004), S/2016/1038 (December 9, 2016), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/1038.

FATF statistics provide further evidence of inadequate implementation, despite the fact that the organization only focuses on U.N. financial sanctions on North Korea and Iran. FATF standards are assessed on a five-part scale:

- C: compliant
- LC: largely compliant; only minor shortcomings
- PC: partially compliant; moderate shortcomings
- NC: non-compliant; major shortcomings
- NA: not applicable. A requirement does not apply, due to the structural, legal, or institutional features of the country.

The effectiveness of implementation on these standards is measured by "immediate outcomes" on a four-part scale:

- HE: high level of effectiveness; the immediate outcome is achieved to a very large extent; minor improvements needed.
- SE: substantial level of effectiveness; achievement to a large extent, with moderate improvements needed.
- ME: moderate level of effectiveness; the outcome is achieved to some extent, but major improvements are needed.
- LE: low level of effectiveness; the immediate outcome is not achieved or only to a negligible extent, with fundamental improvements needed.

To date, 65 states have been evaluated against the 2012 FATF standards, which include Recommendation 7 (the North Korea and Iran targeted financial sanctions) and Immediate Outcome 11 (which demonstrate whether or not the implemented targeted financial sanctions were effective). These scores are shown in Table 2.

These data show that even against FATF's limited requirements on proliferation financing, states are inadequately meeting these standards both in terms of technical compliance and effectiveness.

The next two sections will outline the prevailing legal regimes in key national jurisdictions: the United States and a few other states. A survey of these legal regimes reveals a number of important factors. To begin with, countering proliferation finance sits at the intersection of several different legal and regulatory approaches, with different departments responsible for understanding and combating different aspects. This fact often leads to no single agency taking leadership and ultimate responsibility for a coordinated and comprehensive national approach to the issue.

On the one hand, a multi-agency involvement in the issue can be an advantage for building a stronger regime, as it increases the tools and resources that can be brought to bear on the problem. On the other hand, it also means that there are interagency "stovepiping" obstacles to closer cooperation. For example, both the Department of Defense and Department of State operate technical assistance programs run by the Defense Threat Reduction Agency for Defense and by the Export Control and

TABLE 2

Cumulative Scoring of States against the 2012 FATF Standards

TECHNICAL COMPLIANCE	COMPLIANT	LARGELY COMPLIANT	PARTIALLY COMPLIANT	NOT COMPLIANT
NO. OF COUNTRIES	10	14	21	20
EFFECTIVENESS	HIGHLY EFFECTIVE	SUBSTANTIAL LEVEL OF EFFECTIVENESS	MODERATE LEVEL OF EFFECTIVENESS	LOW LEVEL OF EFFECTIVENESS
NO. OF COUNTRIES	2	14	17	32

Source: Financial Action Task Force, "Consolidated assessment ratings," (November 26, 2018), http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf.

Related Border Security (EXBS) for State. U.S. partners who have worked with both programs rate the level of assistance as high quality. However, the two programs, according to experts, do not often communicate on proliferation finance priorities.

Beyond the national coordination issue, there are distinct groups of leaders and laggard states with regard to efforts to counter proliferation financing. The distinctions between the two – what makes one state capable and eager to fight the threat and another not – are important if the international community is to build an effective consensus and competency around fighting proliferation threats.

The Legal Regime in the United States

The United States is a leader on countering proliferation finance due to its relatively strong existing statutory prohibitions and authorities, and the model it offers to other jurisdictions on how to address the issue. The United States is rare in having been rated highly effective in implementation of United Nations targeted financial sanctions on DPRK and Iran by FATF. However, the U.S. system features serious vulnerabilities as well that have allowed proliferators to take advantage of the system. These include challenges in banking regulations and the problem of anonymous companies, especially the extent to which the United States does not mandate the collection of beneficial ownership information, which refers to the individual who actually controls a corporate entity, even though the entity may not legally be in that person's name.

Broadly, the United States has one of the most well-developed legal and regulatory frameworks when dealing with financial crimes compliance issues. However, even these impressive capabilities do not fully incorporate proliferation finance as explicitly as the threat requires. In the United States as in the United Kingdom – two of the leading jurisdictions in countering proliferation finance efforts – efforts against proliferation finance have failed to come into their own as a distinct area of law. The financing of proliferation is not explicitly criminalized. Rather, countering proliferation finance is largely governed indirectly via three regulatory regimes: export control, sanctions, and anti–money laundering. This deficiency lowers its profile as a risk compared with countering terrorist financing. By comparison, while financing terrorism is a specific criminal offense, proliferation finance can be addressed only sideways using these three regulatory frameworks – none of which captures the full scope of proliferation finance alone, thereby contributing to the problem of willful blindness.

Before outlining what changes would be needed to more fully address the financing of proliferation, it is worth explaining how the existing U.S. legal framework, particularly export control, sanctions compliance, and anti–money laundering measures, treat the money-making and movement of proliferation networks. By sketching this legal framework, this section provides a snapshot of the current national patchwork of countering proliferation finance law. At the center of these three regulatory structures sit financial institutions, which have the potential to act as the first line of detection and denial when proliferators engage with the financial system. This is a necessary aspect of their work, as well as being a potential chokepoint to disrupt their activities, which

The Trump administration, concerned that Iran will return to a nuclear-enrichment path that may include a weaponization component, has used diplomatic and economic tools to constrain Iran's abilities to do so. Iran's Army Day parade showcases examples of Iran's sophisticated missile capabilities. (Majid/Getty Images)

underscores why proliferation finance is important and distinct from larger countering proliferation efforts. Banks can uniquely contribute through their knowledge of customer transactions. They must extend the work they already do to meet regulatory and legal requirements – and their regulators must better incentivize such activity. Like proliferation finance networks, financial institutions are transnational, with asymmetric influence, by comparison with national governments, to stem financial flows. However, that influence does not translate automatically into effectiveness. Too often financial institutions, even when aware of the proliferation threat, remain enablers of proliferation finance by acting as unwitting gatekeepers into the formal financial system. Awareness-raising, capacity-building, and technical assistance can ameliorate this situation, along with greater requirements for the sellers and shippers of proliferation goods. But political will, as this report emphasizes in a later chapter, must also be present for the entire system to work properly.

Facilitating the countering of proliferation finance presents a significant regulatory compliance risk for banks.

As a number of bank representatives emphasized in interviews with the authors of this report, financial institutions' obligations in the countering proliferation finance space are not black and white, particularly because the issue cuts across regulatory frameworks but lacks its own. For example, many banks approach proliferation finance efforts using the same perspective they take with sanctions screening. That is an incomplete foundation, however, as proliferation networks continuously create new entities to conduct illicit activity. These firms would be designated only after they had been caught conducting proliferation activity.

Other banks use strategies for dealing with money laundering threats to combat proliferation finance. While such strategies may help in thinking about how to collect data from commercial account holders involved in deceptive trading practices, money laundering and proliferation finance are distinct threats. Money launderers are trying to clean dirty money; proliferators want to move clean money in order to obtain goods illegally. More advanced banks recognize the need to build on their detection and investigation methods from anti–money laundering to tackle proliferation finance.[22]

For banks, facilitating the countering of proliferation finance presents a significant regulatory compliance risk. Their approach to detecting and reporting proliferators in their networks is informed by limited formal, as well as informal guidance from governments; the legal and regulatory frameworks outlined below; and their own appetite for risk. Many banks interviewed by this research team expressed a desire for clearer regulations and guidance (both public and, to avoid adaptation by the networks themselves, private) outlining their obligations regarding countering proliferation finance. More expansive regulations can offer a much stronger proliferation control regime, in which export controls, sanctions, and anti–money laundering work can be more aggressively targeted to better discover and disrupt proliferation networks.

In May 2017, a U.S. federal judge approved "damming" seizure warrants for North Korean money in some of the United States' and the world's biggest banks, which included Deutsche Bank. (Thomas Lohnes/Getty Images)

An additional weakness of the U.S. approach is the idea that expanding the legal regime around proliferation finance in the United States will be costly and have a negative impact on companies. It is true that the compliance divisions of international banks represent a significant cost center to their broader enterprises. However, focusing solely on the costs of additional regulatory scrutiny, not its benefits, is shortsighted. Companies are already paying costs of compliance by trying to do due diligence without having proper guidance about what the right flag posts and standards should be. It is in banks' interest to have a stronger and more efficient regulatory posture. Otherwise, the risks and costs are uneven and spread around banks and companies. Indeed, some of the biggest banks who are keenly aware of their vulnerabilities articulate this perspective themselves.

Many bankers, public officials, and analysts think the current system is deeply flawed and the United States is vulnerable. Former Deputy Assistant Attorney General and current Financial Crimes Enforcement Network (FinCEN) Director Kenneth Blanco has emphasized the ease with which sanctioned entities in North Korea were able to pass money through the U.S. financial system, for the direct benefit of North Korea's weapons of mass destruction program.[23] In one example from May 2017, a federal judge approved "damming" seizure warrants—which are used to block outgoing funds transfers—for North Korean money in some of the United States' (and the world's) biggest banks: Bank of America, Bank of New York Mellon, Citigroup, Deutsche Bank, HSBC, J. P. Morgan Chase, Standard Chartered, and Wells Fargo.[24]

U.S. Secretary Wilbur Ross's Department of Commerce houses the Bureau of Industry and Security (BIS), which modifies the Controlled Commodities List of items whose export and re-export is controlled by BIS. (Win McNamee/Getty Images)

EXPORT CONTROLS

The U.S. export control system is a highly sophisticated web of authorities and statutes that play a key role in preventing the export of goods and technology related to weapons of mass destruction. Included in its purview are dual-use goods, which are primarily commercial and industrial items that could be used for either benign civilian purposes or military activities, including WMD program development. For example, in the 2015 case of *U.S. v. Hsien Tai Tsai*, the Department of Justice sentenced the defendant to 24 months in jail for exporting, without a license, rotary surface grinders from the United States to Taiwan with the ultimate destination of North Korea; these devices can be used to produce rings and gaskets, as well as rocket parts. Tsai had previously been designated for assisting North Korea's weapons of mass destruction program.[25]

The export control system integrates international export control regimes of which the United States is a member. These include the Nuclear Suppliers Group, Missile Technology Control Regime, Wassenaar Arrangement, Australia Group, and Zangger Committee. Within the United States, the implementation of the mandates of these regimes is split among several federal agencies: the Department of Commerce, Department of State, Nuclear Regulatory Commission, Department of Energy, Department of Treasury, and Department of Defense. The Department of State implements the International Trade in Arms Regulations, which controls non-nuclear defense technologies; the Nuclear Regulatory Commission implements nuclear product-specific export controls. The focus of these export control regimes is on exporters rather than banks, but there are legal implications for banks within the regulatory structure.

The U.S. export control system is a highly sophisticated web of authorities and statutes that play a key role in preventing the export of goods and technology related to weapons of mass destruction.

The export control regime of particular relevance in the counterproliferation context is the Export Administration Regulations (EAR), which is administered by the Commerce Department's Bureau of Industry and Security (BIS). The regulations' statutory authority originally derived from the now-expired Export Administration Act, which has been continued under the International Emergency Economic Powers Act. The EAR focuses on dual-use goods with predominantly commercial applications included on the Controlled Commodities List (CCL), a sprawling inventory of specific items whose export and re-export is controlled by BIS. Nuclear materials and chemical and biological weapons are all categories of these controlled items, but the list also covers industrial technology and components that could be repurposed for nuclear proliferation.[26]

Items not specifically listed on the CCL are still subject to the EAR: any item that is in the United States or originates in the United States (among other, more technical, specifications) is considered subject to the regulations. Exporters can determine whether a license is required for their item by identifying it on the CCL and comparing the classification number to a country chart that specifies the receiving countries for which that class of good

requires a license. A dual-use good with nuclear proliferation uses, for example, may be exported to Canada without a license, but not to Pakistan. In this way, the U.S. dual-use export control system monitors goods across two axes, taking into account both the risks of a particular item and its final destination.

The EAR includes general "catch-all" provisions (called EPCI, the Enhanced Proliferation Control Initiative) that significantly expand controls over proliferation-supporting activities. EPCI broadens U.S. export controls based on exports' end use, expanding EAR beyond simple list-based control. In Part 744.2, entities are prohibited from exporting, re-exporting, or transferring any item subject to EAR without a license that the exporter has knowledge (defined as to "know or have reason to know") will be used for nuclear explosive purposes or other illicit nuclear ends.[27] This provision expands the Commerce Department's authority to include any item – as long as it originated or exists in the United States – that is known to be destined for proliferation. Part 744.6 is of particular relevance to proliferation financing: it prohibits any U.S. person from knowingly supporting an export, re-export, or transfer of an item that has a proliferation-related end use. Support is defined to include financing.[28]

Banks are obligated to conduct due diligence and keep records of transactions concerning dual-use goods in their trade finance businesses. However, it does not appear that the Commerce Department has ever brought an enforcement action against a bank for failing to do so, and many bankers told this report's research team about the difficultly in keeping up with additions to export control lists. For banks, finding these listed goods among documents related to their purchase, sale, or transfer requires a granular knowledge of what is being shipped that is not available to banks handling the trade finance aspect of the transaction. This is true in large part because the way in which goods are labeled (on payment invoices, for example) does not often provide sufficiently detailed information to allow checking against what would appear on an export control list. Additionally, many banks have said they lack the expertise to vet export control lists.[29]

Another challenge is that many jurisdictions do not digitize trade finance documents. This makes it difficult for banks to quickly verify information about commercial transactions. As trade is increasingly conducted via "open account" terms – in which the buyer and seller do not rely on the bank for any crediting – banks are losing the visibility into transactions that trade finance traditionally provided.[30] A bank can still conduct standard sanctions screening against the parties involved in an open-account deal, but their ability to see the underlying reasons for the transaction, because of limitations in the amount of information a Society for Worldwide Interbank Financial Telecommunication (SWIFT) message can convey, is sharply curtailed.

The lack of visibility into transactions is a serious vulnerability for broader counterproliferation efforts.

This is a serious vulnerability for broader counterproliferation efforts: it is hard for banks to see the full spectrum of trade data, and it is difficult for customs, shipping agents, freight forwarders, and the wider shipping community to spot a suspicious money trail in the movement of goods. Currently, financial payment information available to banks generally offers extremely limited information about the details of a financial transaction. This is especially true in the trade space, where the payments are for goods, but banks cannot verify a lot of the information about what the goods are or their ultimate end use. Only 20 percent of global trade is conducted with trade finance, which requires greater disclosure of information about the transaction for the banks processing it.[31] The rise of the alternative open-account transfer is more prevalent, and ultimately features less transparency for the banks that are trying to scan transactions for proliferation-related goods. Expanding required information in financial payments would facilitate the collection of information that may help banks identify proliferation networks.[32]

U.S. SANCTIONS REGIME

The United States layers its own domestic sanctions authorities on the international nonproliferation sanctions regime of the United Nations, deepening the compliance obligations that national authorities place on banks beyond U.N. requirements. U.S. sanctions prohibit a broader range of activities and entities than do U.N. sanctions (for a comprehensive list, see Table 3: Executive and Legislative Actions That Form the U.S. Sanctions Framework Related to Proliferation). Domestic sanctions authorities can be developed by the executive or legislative branches, with executive orders primarily deriving their authority from the International Emergency Economics Powers Act. Legislative sanctions often address country-specific risks, for example

the North Korea Sanctions and Policy Enhancement Act of 2016. Most sanctions are implemented and administered by the Office of Foreign Assets Control (OFAC), which is within the Treasury Department and has the authority to designate entities, issue regulations, and conduct enforcement actions. The State Department also has the authority to designate entities and coordinate with OFAC in issuing sanctions guidance.

In addition to screening clients against sanctions lists, U.S. banks are advised to take risk-mitigation measures that ensure they do not inadvertently finance (1) designated entities hiding behind shell or front companies or (2) any proliferation activity by designated entities pursuant to WMD authorities.[33] Due diligence is required to make sure that banks freeze the assets of not only persons on the Specially Designated Nationals and Blocked Persons list, the U.S. sanctions blacklist, but also, generally, of entities owned or controlled by them. This poses a dilemma, though, when financial institutions do not have access to accurate or up-to-date details on who owns or controls a company (i.e., beneficial ownership information), because the jurisdiction in which they operate does not require its collection and disclosure in the corporation formation process.

This is embarrassingly the case in the United States, which FATF has graded as non-compliant for its failure to mandate beneficial ownership disclosure.[34] Despite entreaties to legislators from law enforcement and the banks themselves to patch this hole, congressional efforts to do so have consistently stalled. As long as that remains the case, it is almost certain that North Korean money is making its way through the U.S. financial system, obscured from the gaze of sanctions screening, as in the previously cited "damming" seizure warrants for banks processing more than $700 million in transactions on behalf of entities tied to North Korea.

Banks are also accountable for the broader activity-based sanctions embedded in international and domestic frameworks (including UNSCRs such as 2397, which restrict certain types of energy trade with Pyongyang, and Executive Order 13810) banning, for example, transactions that raise hard currency for North Korea via natural resource sales.[35] Despite the broad mandate of these sanctions, their enforcement on financial institutions so far has been limited, mostly to banks that were found to be transacting with entities already designated by sanctions. So far, Commerzbank AG, HSBC, and BNP Paribas are among the financial institutions that have been prosecuted and/or subject to civil enforcement under sanctions law for intentionally creating payment systems that omitted or obscured information to evade U.S. sanctions on proliferators.[36]

ANTI–MONEY LAUNDERING REQUIREMENTS

While proliferation financing is an area of lesser focus for many regulators and banks, money laundering is a familiar crime already subject to sophisticated legal frameworks. U.S. law does include financing of proliferation as a subset of the crime of money laundering, so many banks and regulators may believe that anti–money laundering compliance will also minimize banks' involvement in proliferation finance.[37] Consequently, components of countering proliferation financing practices at banks – such as flagging, investigating, and filing suspicious activity reports (SARs) on transactions of concern – originate in anti–money laundering programs.

However, effective anti–money laundering controls are not sufficient to combat proliferation finance: unlike money laundering, which tries to hide the origins of dirty money, proliferation financing involves raising money that is likely to support a weapons of mass destruction program, and that hides the purpose of the goods being purchased with often legitimate money. The typologies of proliferation finance differ from money laundering in a number of ways, including that the former often involves legitimate transactions at the front end.[38] Despite the shortcomings of anti–money laundering programs in the context of countering proliferation finance, they remain one of the most robust legal frameworks that apply to this nascent compliance space.

In the United States, the most important anti–money laundering statutes that create obligations for banks are the Bank Secrecy Act (BSA) of 1970 and Title III of the

Effective anti–money laundering controls are not sufficient to combat proliferation finance.

USA Patriot (Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001, which significantly amends the BSA. Certain obligations and protections created by these statutes – such as filing SARs and safe harbors for companies to share information without legal liability for allowing past illicit conduct by customers – play a key role in banks' countering proliferation finance compliance work as well.

Under the Bank Secrecy Act, banks are required to undertake risk-based procedures for conducting customer due diligence and ongoing monitoring of accounts in order to report suspicious transactions. Banks are required to verify customers' identity before opening an account.[39] Banks must also submit SARs for any activity that might violate the law, or for any

TABLE 3

Executive and Legislative Actions That Form the U.S. Sanctions Framework Related to Proliferation

EXECUTIVE ORDERS

General nonproliferation actions

E.O. 12938 (1994): Underpins the general nonproliferation sanctions regime not specifically tied to a particular state. Prohibits the importation of goods or services provided by anyone found to be supporting proliferation activity.
E.O. 13094 (1998): Amends E.O. 12938 to include additional measures that should be taken against a foreign person determined by the Secretary of State to be contributing to any entity's WMD proliferation program. Those measures include a ban on federal government procurement from or assistance for the designated person, as well as a ban on importing any goods or services produced by the person.
E.O. 13382 (2005): Provides for the blocking of persons who have been designated as engaging in or supporting proliferation, and gives the Treasury Department the discretion to also block any persons financially supporting those listed.

North Korea nonproliferation actions

E.O. 13466 (2008): Declares a national emergency due to the threat of proliferation of WMD on the Korean Peninsula and transfers existing sanctions from the authorization of the Trading with the Enemies Act to the International Emergency Economic Powers Act, which authorizes the majority of contemporary sanctions.
E.O. 13551 (2010): Expands the scope of the national emergency related to North Korea declared by E.O. 13466, creating authority to block property and assets of listed persons pursuant to U.N. Security Council Resolutions 1718 and 1874.
E.O. 13570 (2011): Expands the scope of the national emergency related to North Korea in the previous executive orders, strengthening the Treasury Department's authority to implement U.N. Security Resolutions 1718 and 1874. Prohibits the importation of any goods from North Korea.
E.O. 13687 (2015): Implements U.N. Security Resolutions 2087 and 2094 by expanding the list of U.S.-blocked persons related to North Korea.
E.O. 13722 (2016): Implements U.N. Security Resolution 2270 and the North Korea Sanctions and Policy Enhancement Act. The order grants Treasury broad authority to designate persons involved in the North Korean economy whose revenue may indirectly contribute to the North Korean government, as well as those providing financial services to them. This order, in tandem with E.O. 13382, underpins the Treasury's imposition of secondary sanctions on Chinese and Russian firms in August, October, and November 2017 and August 2018.
E.O. 13810 (2017): Implements U.N. Security Resolutions 2321, 2356, 2371, and 2375 by giving Treasury the discretion to block any person operating in a range of commercial sectors in North Korea, among other activities, and those who provide financial services to them. The Treasury Department is also given the authority to impose sanctions on a foreign financial institution that knowingly violates sanctions, vastly expanding U.S. authority to impose secondary penalties. This order underpinned the imposition of such secondary measures on two Chinese firms in January 2018.[38]

Principal Iran nonproliferation actions

Note: A broad set of executive and legislative authorities target Iran's threatening and destabilizing activity; these are not listed here. This table lists authorities tied specifically to Iran's illicit proliferation activities.[39]

E.O. 13599 (2012): Implements secondary U.S. sanctions on Iran's Central Bank for concealing transactions between sanctioned parties. This blocks any U.S.-based assets of entities owned or controlled by the Iranian government, in part because of "the threat to government and financial institutions resulting from the illicit activities of the Government of Iran, including its pursuit of nuclear weapons."
E.O. 13716 (2016): Revokes E.O. 13574, 13590, 13622, and 13645; amends E.O. 13628; and provides for implementation authorities of sanctions outside the scope of the JCPOA.
E.O. 13846 (2018): Reimposes Certain Sanctions With Respect to Iran: Reintroduces measures that had been lifted by the JCPOA, with specific reference to countering a range of Iranian threats, including "Iran's proliferation and development of missiles."

ACTS OF CONGRESS

Chemical and Biological Weapons Control and Warfare Elimination Act (1991): Gives the president the authority to use the U.S. export control system to prevent the export of goods and technologies that would assist a country in developing the capability to produce or use chemical or biological weapons. Amends the Arms Export Control Act to establish a list of goods and technologies that would assist a foreign government in acquiring chemical or biological weapons.
Iran Sanctions Act (1996): Enacts sanctions authorities to target firms that sell to Iran any technology useful for its nuclear program or certain types of conventional weapons. The act also sanctions firms that invest in Iran's energy sector.
Iran, North Korea, and Syria Nonproliferation Act (2006): Authorizes the United States to impose trade sanctions on individuals and entities – not just governments – that engage in proliferation.
Comprehensive Iran Sanctions, Accountability, and Divestment Act (2010): Amends the Iran Sanctions Act to expand the energy-related activities relevant to Iran that are sanctionable and to add measures that can be imposed. The act also mandates the imposition of sanctions on foreign financial institutions that facilitate WMD transactions related to Iran, among other activities.
Iran Threat Reduction and Syria Human Rights Act (2012): Broadens the Iran Sanctions Act by requiring sanctions to be imposed on non-U.S. firms directly or indirectly involved in specified activities, particularly in relation to the provision of vessels and shipping services to transport certain goods related to proliferation or terrorism activities. U.S. firms can also be liable for the actions of their foreign subsidiaries that violate sanctions against Iran.
Iran Freedom and Counter-Proliferation Act (2012): Imposes sanctions on persons connected to Iran's energy, shipping, and shipbuilding sectors, as well as on those transacting in precious metals or materials that could be used in Iran's WMD or ballistic missile program. Financing any of these activities is also prohibited.
North Korea Sanctions and Policy Enhancement Act (2016): Requires the president to impose sanctions on anyone supporting or engaging in proliferation activities. Previously this was at the discretion of the president, in tandem with the Treasury and State Departments. This act also widens U.S. authority to impose secondary measures.
Countering America's Adversaries through Sanctions Act (2017): Imposes sanctions on Iran, Russia, and North Korea pursuant to an array of threats, including, in the case of North Korea, proliferation activity. It updates the North Korea Sanctions and Policy Enhancement Act to include subsequent U.N. Security Council sanctions; prohibits indirect correspondent accounts; and enhances inspection authorities to enforce North Korea–related sanctions.

customer activity that is abnormal for that person's profile and has no clear business or lawful purpose. In addition to flagging potential instances of money laundering, these SARs can be used to flag proliferation-related activity – even though banks interviewed by this research team expressed difficulty in differentiating suspicious activity linked to proliferation from other suspicious activity and difficulty in identifying proliferation financing at all. Indeed, U.S. government officials interviewed for this report said that the utility of specifically flagging proliferation finance as the reason for a SAR was of dubious value, although that may be a function of the sophistication of the U.S. jurisdiction. It may be valuable for national authorities in other, less mature jurisdictions to have their financial institutions flag proliferation-linked transactions, in order to raise awareness within the compliance community as to the importance of looking for these red flags.[40] What matters is that the SAR is filed in the first place, and that as much descriptive information as possible about the transactions and account holders is included.

Current and former members of the law enforcement community told the authors of this report that knowledge of a possible proliferation transaction is not usually what initiates a broader investigation, but it is an important piece of data for mapping a network and has figured in previous proliferation cases.[41] Such reports may initiate a probe and can certainly have value in ongoing investigations that have been launched with a predicate offense of money laundering or violation of trade controls.

The Patriot Act amended and strengthened the BSA to require U.S. financial institutions to apply enhanced due diligence to correspondent banking accounts, which are any account established for conducting transactions with a foreign financial institution. The Patriot Act also required banks to apply enhanced scrutiny to accounts held by senior foreign political officials, known as politically exposed persons. Because of their role in cross-border payments, correspondent accounts virtually always factor into proliferation finance pathways:

North Korea, for example, is known to commonly use correspondent accounts with Chinese banks to facilitate international transactions.[42] The amended BSA made anti–money laundering measures even more applicable to countering proliferation finance efforts by placing them under greater scrutiny.

The Patriot Act includes provisions under Sections 314(a) and 314(b) to encourage and allow information sharing between banks and the federal government regarding potential money laundering and terrorist financing activities. Under these provisions, the U.S. government is able to query banks for specific information, through FinCEN (and receive other information from banks), and banks are given certain liability protections to share information with one another regarding money laundering and terrorist financing. The sharing of proliferation finance information is broadly, though not universally, considered to be swept into the authorities for money laundering information exchange. A more explicit legal reference about its inclusion could enhance information exchange on this topic, encouraging banks to focus more on it because their regulators would be given a more explicit focus on it.

Recently, the Treasury Department has taken increased advantage of Section 311 of the Patriot Act to counter proliferation finance. Section 311 allows the Treasury Secretary to designate a foreign jurisdiction, account, or financial institution as being of primary money laundering concern. This designation allows the Treasury to require domestic financial institutions to take special measures in relation to the designated entity, such as additional due diligence or limitations on the opening of correspondent accounts. In practice, given the salience for all major international institutions of abiding by U.S. law, this means a 311 designation can have a crippling effect on a target.

Former U.S. President George W. Bush speaks about the Patriot Act at the National Counterterrorism Center. The act significantly amended the Bank Secrecy Act of 1970, creating certain obligations and protections that play a key role in banks' countering proliferation finance compliance work. (Mark Wilson/Getty Images)

The first, and most prominent use of the 311 authority against a proliferator was in 2005, when the United States designated Banco Delta Asia as an institution of primary money laundering concern, acting specifically on behalf of North Korea.[43] In 2016, the United States designated North Korea as a jurisdiction of primary money laundering concern and prohibited U.S. financial institutions from opening correspondent banking accounts on behalf of North Korean banks. U.S. financial institutions are required to conduct enhanced due diligence to make sure North Korean entities are not gaining access – even indirectly – to U.S. correspondent accounts.[44] The Treasury Department also used the 311 authority to designate the Bank of Dandong as of primary money laundering concern for violating U.S. and U.N. sanctions on North Korea in November 2017, effectively cutting the Chinese bank off from the U.S. financial system.[45] In early 2018, FinCEN pursued a 311 action against ABLV, a Latvian bank that had facilitated North Korean financial transactions in violation of U.S. and U.N. sanctions.

A Section 311 designation allows the Treasury Department to require domestic financial institutions to take special measures in relation to designated entities.

FOREIGN LEGAL REGIME: LEADERS AND LAGGARDS

While the United States has been an effective standard setter, it is not the only major international player that has implemented a powerful legal and regulatory framework for countering proliferation finance. However strong or weak the international frameworks established by the United Nations or FATF are, they are translated into laws, regulations, and procedures at the national level, which includes the risk management practices of global banks. The capacity, resources, and will that any one country can bring to bear on this issue vary widely. Strong national-level legal frameworks have some particular themes in common. First, they allow for the fast and efficient imposition of United Nations sanctions, particularly those targeting specific state actors such as North Korea.

Second, like the United States, nations in the top ranks have laws in place to cover export control frameworks, sanctions, anti–money laundering, and other financial transparency measures. FATF has underlined the intertwined nature of countering proliferation finance and export controls in its own reports: "Many of the policy options for countering proliferation finance draw on resources already available through the export control system, or are dependent on information or legal authorities which is available only from export control authorities."[46]

The United Kingdom and Australia are good examples of countries with effective political leadership and technical expertise on proliferation issues that could serve as models for other jurisdictions. They are both major international trading nations and active members of international regimes for the control of illicit goods, including the Australia Group, Nuclear Suppliers Group, Wassenaar Arrangement, and Missile Technology Control Regime.

Australia, in particular, has been recognized for leading legislation on countering proliferation finance. Australia's Charter of the United Nations Act of 1945 provides a legal framework to implement Security Council Resolutions, including those related to proliferation finance. These regulations are then made by the executive branch, but do not have to be passed by parliament, allowing for speedy amendments that can "ensure timely compliance with Security Council Resolutions."[47] Besides an overarching framework for implementing UNSCRs, Australia's parliament also passed related "Regulations on Dealing with Assets, Democratic People's Republic of Korea, Iran, and Customs (Prohibited Exports)." Australia has a profound advantage over the United States, in that its Australian Transaction Reports and Analysis Centre has access to all cross-border transactions, on which they can immediately run analysis. U.S. rules, by contrast, require the collection of data only for transactions exceeding $3,000, and have to request the data directly from banks.

The United Kingdom currently operates under European Union (EU) rules for countering proliferation, though it does have its own regulatory framework for trade controls, and is currently involved in "onshoring" much of the regulatory framework to U.K. law in response to its decision to leave the European Union (for example, by passing legislation granting it the authority to impose sanctions). Much like the U.S. export control system, however, the EU regulation governing dual-use goods includes a catch-all clause (Article 4) requiring exporters and firms providing brokering services to notify and seek approval from national authorities if they are aware that a dual-use good is destined for a WMD-related end use. This clause allows the regulation to include items that are not on the EU dual-use list.[48] In this regulation, "brokering services" excludes financial businesses, differentiating the EU regime from that of the United States by omitting financial service providers from the catch-all provision.

The United Kingdom has a leading framework on proliferation finance. Unlike other jurisdictions, the U.K. criminalizes activities that constitute proliferation finance. (Jack Taylor/Getty Images)

Another important benchmark enshrined in U.K. law is the set of regulations that update previous compliance requirements for banks in detecting and preventing money laundering and terrorist financing. Banks are required to carry out ongoing monitoring and customer due diligence practices, as well as enhanced due diligence in certain high-risk circumstances.[49] Banks must also create anti–money laundering policy statements and keep records of customer due diligence practices. And banks are required to try to identify money laundering or terrorist financing being carried out by their customers, and to alert the National Crime Agency (NCA) with a SAR. Though the regulations were enacted to fulfill the

The United Kingdom and Australia are good examples of countries with effective political leadership and technical expertise on proliferation issues that could serve as models for other jurisdictions.

U.K.'s obligations to implement the EU Anti–Money Laundering Directive, it is unlikely that Brexit will result in any rollback of the regulations due to the U.K.'s independently aggressive stance toward money laundering.

The Proceeds of Crime Act 2002 is the U.K.'s other primary legislation governing anti–money laundering programs, which makes it a crime to fail to disclose information when banks "know or suspect" that money laundering is taking place, an important diligence standard.[50] This statute makes it possible for banks to be held criminally liable for failing to file SARs to the NCA. In 2017, the Proceeds of Crime Act was updated by Section 11 of the Criminal Finances Act, enabling banks to share information among themselves about money laundering activities in order to jointly file reports to the NCA.[51]

Importantly, the United Kingdom, through the Anti-Terrorism Crime and Security Act of 2001, pointedly criminalizes activities that constitute proliferation finance, given domestic law enforcement a powerful legal tool.[52] The United Kingdom also emphasizes the importance of interagency coordination. Sanctions are enforced by the Office of Financial Sanctions Implementation in the Treasury, with assistance from the National Crime Agency (to investigate sanctions breaches), Her Majesty's Revenue and Customs and the Export Control Organization (to enforce trade sanctions), and the Foreign and Commonwealth Office (to negotiate sanctions).[53] Unlike the United States, the United Kingdom also recognized that financial transparency can enable it to meet national security goals. The U.K. government has proposed a public beneficial ownership registry for corporate entities that own or control property in the United Kingdom.[54]

STATE OF THE REGIME IN HIGH-RISK JURISDICTIONS

A number of jurisdictions at a high risk for facilitating proliferation finance, particularly in East Asia, stand out for trying to pioneer solutions, notwithstanding different resource bases and risk profiles. Broadly speaking, they are reasonably well resourced, with technical competency and sophistication as regards tracking illicit financial activity and proliferation activities. Several have shown prominent recent efforts to implement legal authorities and controls around the financing of proliferation. As highlighted by researchers Andrea Berger and Anagha Joshi, Malaysia's Strategic Trade Act imposes severe criminal penalties for export control violations of "strategic items and technology." This act specifically targets individuals and entities involved in financing the acquisition of weapons of mass destruction.[55] The implementing authority in Malaysia, the Ministry of International Trade and Industry, offers continuous guidance and training on the obligations for the Strategic Trade Act for businesses operating in the country.[56] FATF has recognized these efforts, complementing Malaysia for its strong legal and regulatory framework and good interagency coordination, but also encouraging it to improve its framework for using targeted financial sanctions against WMD proliferation.[57]

Thailand is another jurisdiction that has been exploited by proliferation networks – including by entities and individuals who have acted on behalf of North Korea's Ocean Maritime Management (OMM), a North Korean shipping firm known to be involved in arms trafficking.[58] Thailand's Counter–Terrorism and Proliferation of Weapons of Mass Destruction Financing Act of 2016 includes specific and detailed legislation targeting proliferation financing. Notably, the act provides for the immediate listing of persons and entities sanctioned by the United Nations, and specifies criminal liability for a broad range of illicit activity, including:

> providing or collecting funds or conducting a financial or asset transaction or acts in any way to commit a terrorist act or proliferate weapons of mass destruction; acting with the knowledge that the beneficial person of that financial or asset transaction is a designated person; or acting with the intention that the funds or asset are to be used in support of any activity of a designated person or persons, a group or an entity involved in terrorism or the proliferation of weapons of mass destruction.[59]

Conversely, laggard countries that do very little to identify and impede proliferation financing are each weak in their own way. For some countries, there are scant legal prohibitions to fight proliferation finance. This is a foundational problem for many of the least well-resourced jurisdictions. Other countries lack the legal, monetary, and subject matter expertise resources, and need significant technical assistance. FATF, as part of its global review processes, issues public statements about deficient jurisdictions that the body is monitoring, highlighting specific gaps in national laws or implementation. States can graduate from such close and critical scrutiny, exiting monitoring by creating and implementing comprehensive plans to improve anti–money laundering and countering the financing of terrorism (AML/CFT) measures. This can have a beneficial impact on combating proliferation finance as well. However, given the previously described limitations on

the requirements and guidance that FATF and the U.N. set out for countries, a plan for greater national financial transparency and monitoring may yet leave countries inadequately equipped to combat the threat.

Among these "high-risk and other monitored jurisdictions" identified by FATF in its review as of October 2018 are North Korea, Ethiopia, Iran, Pakistan, Serbia, Sri Lanka, Trinidad and Tobago, Tunisia, and Yemen.[60] Not surprisingly, many of these countries are high on the list of jurisdictions about which the international community is concerned for countering terrorist financing, or are active combat zones involving foreign terrorist organizations (Syria, Pakistan, and Yemen). North Korea is an extreme proliferation risk, which unsurprisingly has failed the test for adequate international financial standards. Iran is under enormous scrutiny from the United States for proliferation activity (though FATF's most recent statement on Iran focused on its AML/CFT deficiencies, reflecting the current focus of FATF standards).[61] Pakistan, too, is an extreme proliferation risk because of both its rapidly developing nuclear weapons program and the proliferation activities of A. Q. Khan and his international network, uncovered only in 2003.

For some countries, there are scant legal prohibitions to fight proliferation finance.

For other states with moderate deficiencies, such as China, which was last rated as non- or partially compliant with 25 out of the 40 FATF recommendations, FATF has identified specific legal measures that need to be taken to assure the international community that the countries are improving their frameworks for combating illicit and criminal financial activity (including potential financing of proliferation).[62]

By way of example, in its June 2018 compliance report on global AML/CFT, FATF highlighted the following needed changes to improve financial sector transparency, among a variety of issues: implementing targeted financial sanctions (Ethiopia); improving interagency and federal-provincial cooperation (Pakistan, a noted proliferation risk); ensuring that national authorities have timely access to beneficial ownership information (Serbia); enhancing even the most basic risk-based supervision of financial institutions (Sri Lanka); and encouraging national authorities to pursue prosecutions when criminal cases are made (Trinidad and Tobago).[63]

The cases of India and Pakistan are worth further discussion, and Pakistan is covered in a later case study. There is a clear distinction in how the international community and the United States approach proliferation risk from countries that are under sanctions regimes (Iran, North Korea, and Syria) versus those that are not (India and Pakistan). As will be discussed in the Pakistan case study, sanctions on India and Pakistan were removed for political reasons – the underlying proliferation and acquisition of goods in violation of export control regimes never stopped. The international community simply decided its limited bandwidth was better used against other proliferation threats. It is worth questioning whether that acquiescence has permitted the sustainment of dangerous networks and contributed to an arms race in South Asia that is extremely destabilizing.

POLICY CHANGE: SEIZING THE OPPORTUNITY

Highlighting these specific deficiencies provides a roadmap for the international community to tailor properly its technical assistance work. To be sure, this work is challenging for governments and banks alike as a practical matter, given the breadth of regulatory requirements and resource constraints. That difficulty is only exacerbated, however, by a lack of high-level political prioritization, and by the fact that the international community has not reached consensus on building a true, institutionalized, practical commitment to more information gathering, disclosure, and sharing.

If the U.S. administration wishes to challenge adversaries on nonproliferation priorities, it has no choice but to keep pushing on international standards and national-level compliance related to countering proliferation finance, prioritizing opportunities to advance a more ambitious policy framework. There is a strong possibility that countering proliferation work may be possible even while other nonproliferation issues remain highly controversial, including how to approach Iran's ambitions. The United States has significant ability to shape the issue from Washington, especially by focusing on congressional legislation, and with Treasury officials making the most of leadership opportunities during the U.S. presidency of FATF from 2018 to 2019. Some U.S. officials have embraced this perspective, as evidenced in their agenda document for the FATF presidency, but bandwidth issues, exacerbated by the short duration (one year) of the FATF presidency are significant challenges.[64] This is compounded by the fact that China, which is a drag on leadership on these issues, will assume the FATF presidency in mid-2019.

In its most recent plenary, FATF announced that it was starting a project to gauge the degree of support among

member states for expanding the FATF recommendations for countering proliferation finance and for enhancing the implementation of existing obligations. The project will also consider developing best practices on combating proliferation finance. These may address such issues as criminalization, international cooperation, and how to conduct risk assessments. Unfortunately, it is unlikely that the U.S. delegation will serve as a co-chair for that effort, which reduces the chances of pushing meaningful changes the project team recommends at a future plenary. It is certainly unlikely to happen quickly, while the United States holds the FATF presidency.[65]

The Influence of International Rules on the Private Sector

The private sector must match major steps taken by the government sector if the countering proliferation regime is to work effectively. The private sector responds to the requirements and incentives put in place by their regulators, and to the information that government shares with them to identify and track proliferators. This means that the information and signaling from governments is a crucial function of how effective banks can be at impeding proliferation finance. Regulators in the United States and elsewhere need to signal with concrete legal and regulatory steps that banks must specifically look for proliferation finance, not merely maintain adequate controls against illicit finance. And national governments must lean much further forward in supporting this work by sharing lead information to better identify proliferation finance. Only by adopting this posture will regulators properly balance the costs of economy-wide rules and regulations with the benefits to U.S. national security and actually enable a change in counterproliferation efforts within the private sector.

As governments engage with their banking sectors, they must realize that this is often difficult work for even the most sophisticated financial organizations to carry out correctly and thoroughly on a constant basis. Governments must be prepared to create legal and regulatory frameworks for the greater sharing of information and provision of guidance; otherwise banks will continue to struggle to differentiate proliferation-linked transactions from the much larger volume of legitimate commercial trade they resemble. It is very difficult for global banks to conduct proper due diligence on the customers who are account holders with their correspondent banking partners in high-risk jurisdictions. Ensuring that banks that self-report are not exposed to legal jeopardy is also a crucial step. These positive incentives should exist alongside the threat of fines and legal action.

The Roadblocks: Political Inaction and Inadequate Rules

The most prominent obstacles to a strong countering proliferation finance regime originate in a fundamental lack of political will. This is clearly demonstrated by the very weak, nascent global regime to counter proliferation finance. It may be more accurate to say there are numerous uncoordinated national efforts that attempt to work together, but the whole is far less than the sum of its parts. There is no good public policy reason, aside from a lack of political will to prioritize the issue, to explain inaction on laws and regulation, or why the United States cannot build stronger domestic financial transparency, or has not been more forceful in setting the tone at the U.N. and FATF.

Despite the fact that some legal regimes – in the United States and in some more sophisticated jurisdictions – have developed significant tools to combat the financing of proliferation, the problem persists, with numerous examples of networks operating with ease. The next section analyzes why these problems persist despite clear-cut rules. There are obvious economic reasons for which such activity continues: some states find it lucrative to continue to trade with proliferating states like North Korea. There are also political reasons for why some jurisdictions do not pass sufficiently strong laws (or do not enforce them). Some jurisdictions believe stronger rules hurt business interests, or cracking down on specific bad state actors will have diplomatic consequences. Certain

The most prominent obstacles to a strong countering proliferation finance regime originate in a fundamental lack of political will.

governments have interagency coordination challenges that the highest-level political authorities are not invested in solving. Also, some countries may believe that proliferation finance is a low priority threat, or that proliferation is better addressed through controls on equipment and materials, rather than on related financial transactions. Only stronger political will can overcome the obstacles to a stronger regime.

Proliferation finance experts, as well as representatives of banks and even regulators themselves, have spoken about the need to change legal and regulatory mindsets from a largely rules-based approach to a risk-based one. The hallmark of a rules-based approach is compliance with the letter of the law regarding measures such as the

Cities and provinces in Northeast China create a strong economic conduit between China and North Korea. In Dandong, pictured here, a single company transacted more than $500 million worth of business with North Korea. This situation is replicated throughout the city and neighboring provinces. (Kevin Frayer/Getty Images)

implementation and enforcement of targeted financial sanctions on designated entities. Conversely, a risk-based approach takes a much wider aperture to scrutiny of, in the case of proliferation finance, financial activities undertaken by corporate entities or individuals. A risk-based approach also includes greater surveillance of activity, focused on how account holders conduct their business and structure their transactions, and on who their counterparties are and where they operate.

For a risk-based approach to be implemented, the political and policy community must embrace a much more aggressive posture. The current limited attitude to the issue is an obstacle to better rules, coordinated agency action, measures within and across jurisdictions, and resourcing. It is also an obstacle to basic acknowledgment and coordination among the many constituencies that touch this issue, including nonproliferation, security and defense, financial oversight, and global trade communities. The academic and think tank community has researched the nature of these problems intensely, with numerous studies prominent in the field.[66] Experts have outlined gaps in the regime. It is now up to leaders in national and international forums to translate those ideas into policy. The next two subsections address these political will questions, first within the context of policy decision-making in the United States, and then in the wider international context.

Among the initial challenges for countering proliferation finance regimes in many countries is the overall lack of knowledge about what proliferation finance is and how the specific networks operate in various regions. Often, both the financial institutions and their government regulators lack relevant knowledge of typologies and red flags. More than one representative from a global bank told this report's research team that they felt they were safe from illicit finance originating from North Korea because their customers did not trade with North Korean companies.[67] This is a dangerously restrictive conception of the risk of exposure for financial institutions, because it misses activity that is illegal but would not be captured by sanctions screening alone.

Often, both financial institutions and their government regulators lack relevant knowledge of typologies and red flags.

Just as often, financial institutions know that proliferation finance is a risk, but they lack guidance from regulators about their national and international legal obligations to combat it, how national laws can empower banks to address the threat, and how they can coordinate efforts with other banks in their jurisdiction.[68] Often such an approach exists because national governments and international bodies do not provide adequate guidance themselves. National authorities have often failed to

convey the seriousness of countering proliferation finance as a policy objective, at either the political or the regulatory level. Many banks have uncovered proliferation networks thanks to information about typologies and red flags provided by national governments – however, not every government is proactive or shares enough to clarify the scope of more than one node in a network.

Why do such obstacles exist? Certainly size is not an obstacle: Jersey (in 2011) and the Bahamas (in 2018) have published very respectable guidance on proliferation finance.[69] Many national governments fear that regulatory scrutiny would scare away large classes of customers, and thus do not want to sacrifice their lucrative financial services sectors.[70] Others believe privacy regulations bar them from sharing the kind of information that makes a strong countering proliferation finance regime work.[71]

Virtually all banks in all jurisdictions told this research team that they understood well their legal obligation to file suspicious activity reports. If a U.S. bank believes an account holder is conducting a transaction that is unusual or indicates possible fraud, money laundering, or other illegal activity, it must file a SAR with the U.S. Department of the Treasury's FinCEN, as mandated by the Bank Secrecy Act. Banks in other jurisdictions report SARs to their national authorities, often the financial intelligence units. However, those bankers told this research team that they received neither feedback on whether their reports had been useful to law enforcement, nor guidance on what kind of reporting to regulators would align with highest national priorities for combating financial crime or security threats. As a recent Clearing House report argued:

> As financial institutions have been incentivized by regulatory enforcement actions to file increasing numbers of suspicious activity reports (SARs), a declining percentage provide value to law enforcement. Yet those regulators examining banks for AML compliance continue to emphasize the importance of financial institutions developing carefully crafted, highly detailed SARs, with little to no feedback provide on such submissions, either from themselves or those government authorities who utilize the data.[72]

A much more systemic problem is the extent to which different legal regimes create regulatory islands where information-sharing mechanisms are restrictive. Because individual banks are subject to the laws of the country in which they operate, they often cannot share relevant information about customers with other offices in other jurisdictions but within the same bank. These restrictions make it difficult for large multinational banks to track customer behavior and accounts across multiple nodes in a global supply chain. Realistically, and as extensively documented by open-source investigators such as the Center for Advanced Defense Studies (C4ADS), proliferation networks are global and span multiple institutions and countries, and they involve multiple people.[73]

A culture of restrictions on data sharing out of fear of losing a competitive edge, or of exposure to legal risk, or because of privacy concerns, is an obstacle to the countering proliferation finance regime. Numerous bank compliance officers cited strict privacy regulations as an obstacle to better information sharing on proliferation finance red flags and typologies. This trend is continuing with the European Union's introduction of the Global Data Protection Regulation, which makes it much more difficult for banks to share information.[74] While privacy protections are of course important, they must not become an insuperable obstacle to keep malign actors out of the global financial system. There is a real tension between privacy and the economic interests of the global trade and financial services sector on the one hand, and on the other the interests of the international community in preventing a catastrophic use of a weapon of mass destruction. Proliferation networks count on those gaps to procure dangerous capabilities without having to worry about strict scrutiny or aggressive law enforcement action until they have acquired what they need.

Improving these political will problems becomes more urgent as the nature of global financial systems changes in response to technological changes. The United States and its partners must be well positioned to anticipate changes in financial technology that can impact the utility of crimes investigation and sanctions compliance. While some financial technology innovations, such as distributed ledger technology, may make it easier to increase transparency in payments, others, for example virtual currencies, can make anonymity easier. The rise of peer-to-peer payments in particular presents obstacles to transparency and to the reach of U.S. jurisdiction. To the extent that the United States sits in the loop of global payments that take place in dollars, it can wield its legal jurisdiction to enforce sanctions or other currency-linked controls on proliferation finance.

Political Challenges to Countering Proliferation Finance in the United States

In the United States, even as executive agencies may acknowledge the proliferation finance threat, this theme is broadly absent from the foreign policy approach to the most significant illicit nuclear challenges. The Departments of State, Commerce, Homeland Security, and Justice, and the 17 members of the intelligence community touch on issues involved in tracking proliferation finance. However, they all see different pieces, which makes coordination difficult. As a result, highest-level analytical work to identify and fill gaps and set related policy priorities for national attention is a challenge.

The government role is important because financial institutions ultimately build their crimes compliance strengths around what national authorities incentivize through legal requirements and formal and informal guidance. Proliferation finance is distinct from money laundering or terrorist financing because its indicators – how the money trail winds its way through global banks, what kind of account holders are involved – are different, leaving banks at a decisive disadvantage. Often the transactions underlying a proliferation finance effort look extremely similar to legitimate commerce undertaken by respectable trading firms. Financial criminals often hide behind constantly changing aliases and move money between jurisdictions and currencies, taking advantage of anonymous companies. In practice, a focus on checking a sanctions list for named proliferators only turns up nodes, including long-defunct nodes of proliferation networks rather than current activity.

To robustly track proliferation activities, banks and firms of all sizes must augment sanctions compliance with customer due diligence, transaction monitoring, and network and pattern analysis strategies to ensure that account holders comply with national and international laws. Many of the largest, most well-resourced banks are already doing this, but even they struggle, which is why banks must also collaborate closely with national regulators to share, with appropriate safeguards, information on proliferation networks. The biggest banks actively engage in these activities already, but they may struggle to work collaboratively with other banks, and smaller banks do not have the resources to implement broad programs for countering proliferation finance. Many of these shortcomings can best be addressed by policymakers setting the correct legal and regulatory framework, which is ultimately a function of exercising political will.

Case Study: The Anonymous Company Problem in the United States

There are several significant technical impediments to building out the legal framework for countering proliferation finance efforts in the United States. The legislative changes to do so are not complicated, but they have foundered amidst political differences. For example, the United States has very minimal standards for disclosure of beneficial ownership in the corporate formation process, which means that the country has a major problem with anonymous companies. Among these it is extremely difficult to trace who ultimately controls and benefits from corporate entities. While incorporation is a legitimate business practice, it is also often used to avoid income tax, park overseas money inside the United States, and launder dirty money.

In this legal framework, proliferation networks can create a string of limited liability corporations conducting legitimate business, only to turn around and use that business track record as a cover for procuring sensitive proliferation-related goods. Know Your Customer procedures and customer due diligence practices, which are vital tools to uncover illicit financial activities and networks, and on which there has been important policy advancement during the past few years, are nevertheless impaired if regulators and law enforcement do not have strong transparency around beneficial ownership.[75]

The lack of progress in ending the problem of anonymous companies in the United States is an important case study that illustrates weak U.S. political will to address illicit finance problems, including proliferation finance. There are several reasons for this. First, the existing situation underscores that while the United States is in many regards a leader on countering proliferation finance, including through its legal framework, technical capacity, and willingness to push an aggressive policy agenda in international fora, the nation still has significant vulnerabilities of its own. It is notable that despite the damage and risk that FATF can deliver to jurisdictions when it discloses their deficiencies, a finding of "non-compliant" in its most recent review of the U.S. approach to transparency and beneficial ownership did not motivate the United States to embrace policy change.[76] Nor does it seem to weigh on the minds of U.S. policymakers that close allies such as Australia and the European Union, have established requirements in pursuit of clear financial crimes compliance priorities.[77] The EU, for example, is intent on building upon its strong beneficial ownership requirements through its Fifth Money Laundering Directive, which requires members to make beneficial ownership registers public.[78]

Arguments advanced by business interests about the overburdensome cost of compliance with beneficial ownership reform are the primary impediment to advancing new laws in this area and stamping out corporate anonymity.[79] These include concern that the penalties for incorrect or incomplete disclosure would be onerous, especially when other government agencies, for instance the IRS and the Securities and Exchange Commission (SEC), collect information on corporations already. Unfortunately for U.S. national security or efforts to effectively combat criminal financial activity, these cost concerns appear to be more salient to policymakers. Both law enforcement and banking communities have spoken out about the need for remedial action on financial transparency. M. Kendall Day, when he was Acting Deputy Assistant Attorney General for the U.S. Department of Justice's Criminal Division, testified to the U.S. Senate that "the pervasive use of front companies, shell companies, nominees, or other means to conceal the true beneficial owners of assets is one of the greatest loopholes in this country's AML regime."[80]

The lack of progress in ending the problem of anonymous companies in the United States is an important case study that illustrates weak U.S. political will to address illicit finance problems.

The problem is not restricted to the anti–money laundering space. The same typologies appear in proliferation finance cases. Foreign-based front companies, either started entirely from scratch or repurposed from already existing entities, where the nature of the business activity switches from legitimate to illegitimate, figured in proliferation cases from North Korea, Syria, Iran, and Pakistan.[81] In one of the most infamous recent "serial proliferator" cases, Chinese national Li Fang Wei (also known as Karl Lee) repeatedly created companies to conduct procurement activity, even as his entities were sanctioned by the United States.[82]

Similar activity has been high-profile news with entities located and operating in the United States. Despite the fact that Iran has for decades been the subject of U.S. primary and secondary sanctions, Iranian entities have been successful in penetrating the U.S. financial system. From 2008 to 2013, U.S. authorities targeted front companies acting on behalf of the Iranian Bank Melli, which, through two shell companies, owned an office tower in New York City for nearly two decades. Through a complex structuring of payments, the building acted as an important revenue stream for the country's nuclear program prior to the Iranian nuclear agreement.[83]

A legal remedy for this company anonymity vulnerability would be quite straightforward. FATF stated the problem for the United States: "Beyond [a SEC requirement for entities that issue securities] there is no requirement for other companies or company registries to obtain and hold up-to-date information on their [beneficial owner] or to take reasonable measures to do so."[84] Congress is the body capable of fixing this problem. Legislators have raised the issue in every Congress since 2008, but there is still a lack of political will to pass the legislation, as most attempts have been left to languish in committee. Former Senator Carl Levin and Representative Carolyn Maloney began introducing the Incorporation Transparency and Law Enforcement Assistance Act in 2008; however, efforts to pass that legislation stopped after Senator Levin retired in 2015. Since then, Representative Maloney and Senator Wyden have introduced the Corporate Transparency Act of 2017, and Senator Whitehouse has introduced the True Incorporation Transparency for Law Enforcement Act, or the TITLE Act. Within the past year, the Senate Banking Committee and the House Financial Services Committee have considered this issue, hearing from industry, independent experts, and government witnesses.[85]

Former U.S. Senator Carl Levin (D-MI) and others have unsuccessfully pushed for legislation to require collection and disclosure of beneficial ownership information in the corporate formation process. (Win McNamee/Getty Images)

The counterarguments to stronger requirements around the burdens of beneficial ownership reporting are understandable concerns, however they are overstated and can be spurious. Small and medium-size companies generally do not have a complicated ownership structure, and the burden of filling out one form to disclose it would not be significant. At present, companies shoulder the costs of trying to manage their vulnerability to being abused by criminals, including proliferators, but have limited guidance or benchmarks from authorities. A fairer policy approach would be to make clear beneficial ownership requirements for all companies, thereby more evenly distributing the costs that are already borne by many companies in the economy. The United States could be a leader and model for other nations to adopt similar preventative measures, insulating themselves from risky financial behavior and national security threats.

AN INCOMPLETE, INADEQUATELY ENFORCED GLOBAL REGIME

The question of political will and inadequate prioritization and enforcement is at least as paramount for the international community as it is for the United States. As referenced in the previous sections on legal framework, the international legal architecture begins with the United Nations with respect to formal legal requirements, and with FATF as regards what could be called "soft law" (requirements that have political, economic, and diplomatic consequences if they are not met adequately). However, a lack of political will has continually stymied international efforts. In one example, FATF member states cannot agree on an official definition of proliferation finance, because too many member states thought an official definition would compel restrictions on legitimate commerce.[86] The lack of a universal definition underscores the weak foundation upon which countering proliferation finance efforts rests.

Just as frequently, the gap between the capabilities and motivation of the private and public sectors to address this issue can be quite wide. While U.S. banks are required to have a risk-based program to detect and halt the financing of proliferation, there is no regulatory incentive to actively detect such activity. In most jurisdictions internationally, banks are not practically required to even have a risk-based approach to tracking proliferation finance. This leads most global banks to the inevitable cost-benefit decision to do only what is necessary to follow the law: check their record to ensure that they are not doing business with anyone on U.S. or U.N. sanctions lists.

These concerns are particularly acute for high-risk jurisdictions, where banks and regulators do not have the level of resources or political will that the United States and Western Europe have. Many bank compliance and government regulators highlight deficiencies in the regime, often because the transnational nature of proliferation networks means that the regime as a whole

The lack of a universal definition underscores the weak foundation upon which countering proliferation finance efforts rests.

is only as strong as its weakest member.[87] The irony of the situation is that with increasing attention being paid by U.S. regulators to the problems of correspondent banking, many banks around the world are being forced by their U.S. correspondents to adopt U.S. banking standards. If U.S. regulators required U.S. banks to specifically seek out proliferation financing, the mandate would be passed on to correspondent banks overseas, effectively strengthening the international countering proliferation financing regime.

To be clear, the public policy implication of this is that banks and companies around the world have virtually no incentives from their national authorities to actually seek out proliferation activities and halt them. Only some institutions have the sophisticated analytical capacities to shut down one of the gravest global security threats, and are properly incentivized to so. Often they do so because they have correspondent banking relationships with financial jurisdictions that have much stronger rules, and their correspondent banks require this of them. Others, however, lack resources and technical capacity, and their national authorities have not identified or put into place the correct incentives. In fact, because of the lack of safe harbor provisions in many jurisdictions, they may be penalized if they do turn up indications that they are being abused by proliferators, while they fail to see the entire value chain, or repeated incidences.[88]

Adding to this dynamic, some governments avoid applying strict scrutiny for diplomatic or political reasons.[89] The Russian Federation, for example, has sought to alleviate severe worker shortages by authorizing North Korean laborers to operate inside the country. While recent United Nations Security Council Resolutions 2375 and 2397 are meant to actively curtail this activity, there is no sign that Russia is slowing down. As recounted in a C4ADS report on North Korean

overseas labor, in July 2018, Russian President Vladimir Putin announced that the permits would be extended, despite a Chapter VII Security Council Resolution (Operative Paragraph [OP] 8 of resolution 2397 [2017]) that such activity should be curtailed.[90]

Case Study: China's Enabling of North Korean Proliferation Finance

Despite purported policy concerns related to nuclear proliferation and repeated requests from the United States and other international actors, China has not been forceful in combating proliferation finance. This is particularly concerning because China facilitates the overwhelming majority of North Korean trade and commerce and therefore has a major role in enabling North Korean proliferation. Prior U.S. administrations have publicly expressed the importance of China's place in convincing North Korea to denuclearize, with former Secretary of State John Kerry saying that China could play a "special role" in making the dream of a denuclearized North Korea become reality. The Trump administration has offered many of the same sentiments, asking China to do more to curb North Korea. But frustration that China seems to shield North Korea from punitive measures, perceived as largely due to its own self-interests, obscures the complex way in which China judges its interests and gauges its ability to control lower-level officials in provinces bordering North Korea.[91]

In China, trade with North Korea is an important source of revenue for the neighboring province of Liaoning, where the city of Dandong is located. This is why so many Dandong-based companies have conducted trade with North Korea, thereby violating international sanctions. Among those that have been identified, Dandong Hongxiang Industrial Development Company (DHID), which was sanctioned by the United States in September 2016, transacted more than $500 million worth of business with North Korea.[92] This kind of firm-level commercial activity is replicated in Dandong and throughout Liaoning and the neighboring province of Jilin, as demonstrated by the multiple Chinese businesses that remained open in defiance of recent U.N. Security Council Resolutions and as reported in the *South China Morning Post*.[93] Dandong relies on trade with the Kim regime for 40 percent of its total trade.[94]

It is clear that the most prominent reason for robust commercial activity with North Korea – in violation of sanctions and of Beijing's own purported interest in limiting North Korea's nuclear ambitions – is the economic impetus for provincial officials to generate growth. These officials must achieve growth targets that the central government sets. In order to meet them, provincial and city governments inflate growth numbers, degrade the environment, or, in the case of Dandong, exploit the lucrative and suspect trade with North Korea. In one example of this kind of trade, between 2013 and 2016, a single company, Dandong Dongyuan Industrial Co. Ltd., was able to export in excess of $28 million worth of materials to North Korea, including motor vehicles, electrical machinery, radio navigational components, and other items associated with nuclear reactors.[95] For context, North Korea's total imports were $3.71 billion in 2016, of which 92 percent came from China.[96] While some local government officials may not be fully aware of their enforcement obligations, resulting in uneven implementation of sanctions while achieving their growth targets, in other cases corrupt local officials are happy to pocket the profits of trading with North Korea. Since Xi Jinping came to power in 2013, the Central Commission for Discipline Inspection, the Chinese Communist Party's anti-graft body, has reportedly investigated more than 2.6 million officials and punished more than 1.5 million, including the former vice governor of Liaoning.[97]

China's continued trade with North Korea is also supported by its need to source carbon-intensive energy from outside its borders in order to meet domestic environmental goals. Transportation costs from North Korea are not high, and the coal itself is cheap to import. Starting in 2016, China made combating pollution, especially in the air, a clear priority. Chinese Premier Li Keqiang said in his 2016 *Report on the Work of the Government* that polluters and those who failed to report environmental violations would be "severely punished."[98] In accordance with the Environmental Protection Law, which was passed in 2014, and the environmental standards set out in the 13th Five-Year Plan, China canceled the construction of 103 coal power plants in 2017 alone, reduced the number of working days annually from 330 to 276, and cut up to 1 billion tons of coal production capacity within the next three to five years. These capacity cuts led to China reaching domestic demand for coal through imports – in 2016, China imported 22.5 million tons of coal from North Korea, almost 9 percent of China's total coal imports for that year.

Dandong, a Chinese border city with North Korea, relies on trade with North Korea for 40 percent of its total trade.

A North Korean restaurant worker tries to attract customers in the Chinese border city of Dandong. The United States has sanctioned restaurants that employ North Korean laborers, because these establishments have often been found to be acting as fronts for other North Korean companies to support the development of North Korea's nuclear program. (Kevin Frayer/Getty Images)

For China, looking the other way on trade with North Korea also offers diplomatic dividends. While China has interests in avoiding an armed nuclear confrontation on its border, it also has national interests that prevent it from completely severing commerce with its neighbor. China does not want to see a refugee exodus into its own territory from North Korea. Allowing revenue streams to Pyongyang is a form of insurance that the North Korean regime and state structure will not collapse under severe financial duress, sending citizens fleeing beyond its borders for aid and services. Regime collapse or compromise would also undercut China's clear and longstanding desire to have a substantial physical buffer between China and Western military forces stationed in South Korea. In the instance that North Korea should collapse, or should unify with South Korea, the U.S. alliance presence in South Korea would presumably spread north to China's borders.

The diplomatic dividends extend beyond bilateral relations to the larger international community; trade flows that fund North Korea's nuclear program give China increased leverage as it negotiates with other countries. When China cracked down on illicit border trade at the end of 2017, it harmed the North Korean economy, with exports declining 37 percent. Due to the increased economic pressure from China, as well as additional sanctions pressures and new summit diplomacy with the United States and South Korea, North Korea has yet to conduct further tests of any weapons of mass destruction or their delivery systems.[99] The outsized control that China has over North Korea's economy, and through that on the scope of its nuclear program, also leads China to try to extract concessions from outside actors such as the United States who would like to see North Korea's nuclear program removed. For example, as tensions between the United States and China escalate on the economic front, White House officials have said that formal talks between the two countries on North Korea's denuclearization process have languished. This demonstrates that China has linked trade with the United States to North Korean denuclearization, refusing to use its leverage to stop North Korea from cheating on sanctions.[100]

Factors such as these will always limit the ability of China to exert economic leverage over North Korea. Even after a decade of international and U.S. financial controls on North Korea and 50 years of arms control agreements and treaties, on top of a regime of nuclear-related trade controls and intensive diplomacy dating back to 1993, years passed without China doing more to combat North Korean proliferation. The United States is in a position to take measures such as unilateral sanctions to hold other countries to account for blatantly abetting Pyongyang, but it has not, until recently, called out China for such activity. Even now, there is far more Washington could do to demand full disclosure of and create consequences for Chinese facilitation of North Korean proliferation activities.

For China, looking the other way on trade with North Korea also offers diplomatic dividends.

These trends are worth watching as the country's economic strength continues to grow. China helped develop Pakistan's nuclear and missile programs, and exported sensitive technologies and materials to countries such as Iran, Libya, North Korea, and Saudi Arabia.[101] If China decides to increase exports to the Middle East, it will use rail linkages through Belt and Road Initiative recipient countries in Central Asia, as many of them house WMD materials. Additionally, the

region is a possible transit node for parts and materials that originate elsewhere, due to the perception that its export and border control systems are inadequate for tracking and controlling the movement of parts across borders.[102] While proliferation finance networks have traditionally turned to manufacturers in the United States and Western Europe for their high quality manufacturers, the domestic upgrade of the Chinese defense industry could lead to other nations looking to Chinese manufacturers. This may implicate more Chinese firms in future proliferation efforts.

More generally, political leaders across the world have been and continue to be willfully blind to the enormous impact of a potential nuclear incident and their complicity in enabling this. Like China, they may have domestic economic self-interests that are more salient to political officials than North Korea's denuclearization. Such self-interests may similarly cause them to actually abet and indirectly and directly support North Korea. Proliferation finance and facilitation of North Korean sanctions circumvention is not just a regional problem – it touches upon every other continent, including Africa.

Case Study: An Illicit Economic Relationship between Ethiopia and North Korea

North Korea and many countries in the Horn of Africa and elsewhere in Africa have economic relationships that date back to the latter decades of the Cold War. North Korea's role as a cheap source of military goods fueled conflicts in the region during the 1970s, but also cemented bilateral relationships that have persisted through Pyongyang's most recent international ostracism.[103] This includes defense relationships with countries such as Ethiopia, where the

During Xi's visit to the Middle East in July 2018, China upgraded its relationship with the Middle East to a "strategic partnership." China has a pattern of supporting the development of Middle Eastern countries' domestic nuclear and WMD programs. (Whang Zhao/ Getty Images)

partnership has also extended into other sectors, for example construction. Successive United Nations Panel of Experts reports, as well as press coverage, have documented a mutually beneficial economic relationship.[104]

Ethiopia helps provide North Korea with essential revenue, much of which goes to its military, supporting weapons of mass destruction research and development through purchasing DPRK goods and acting as a conduit between North Korea and other African countries. The 1718 Sanctions Committee's (DPRK) 2017 annual report revealed a July 2016 interception of an air shipment of 45 boxes of military radio communications products and accessories from China to Ethiopia. Some of these products were labeled as being produced by Glocom, the Global Communications Company. The panel determined

Successive United Nations Panel of Experts reports, as well as press coverage, have documented a mutually beneficial economic relationship between Ethiopia and North Korea.

that while Glocom is based in Malaysia, it is actually a front company for the North Korean company Pan Systems Pyongyang Branch, which finances the North Korean WMD program.[105]

Ethiopia also commissioned Mansudae Overseas Project Group of Companies to build the Tiglachin Monument, which honors Ethiopian and Cuban soldiers who fought in the Ogaden War.[106] Mansudae is sanctioned by the U.S. Treasury Department and the United Nations for engaging in or facilitating the exportation of North Korean workers to generate revenue for North Korea, whose Munitions Industry Department uses part of the revenue to support North Korea's WMD program. Ethiopian Airlines, which is state-owned, has also been reported to have helped transport arms-related materials from North Korea to the Republic of the Congo, thereby violating U.N. sanctions.[107] These willful violations arise in part because countries like Ethiopia find North Korea to be a reliable, low-cost partner, particularly in the defense sector.[108]

Aside from the positive financial incentives to work with North Korea, another problem is that Ethiopia lacks the infrastructure and the political will to implement a legal framework or procedures related to proliferation financing. When FATF evaluated Ethiopia in 2015, it said that it had "not established a legal framework for

the implementation of targeted financial sanctions relating to the financing of proliferation," and rated it non-compliant with Recommendation 7 for this reason: Ethiopia had nothing in place "to comply with UNSCRs relat[ed] to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing."[109] In the same report, FATF noted that it was "unlikely" that Ethiopia was used as a jurisdiction to support proliferation activities outside of the country. As evidenced by these examples, Ethiopia is a nexus for sanctions evasion by North Korea, which should be a much more significant concern for the international community. Since 15 percent of the Kim regime's overall state budget is dedicated to military spending and only 26 percent of the state budget comes from domestic sources, international policymakers should assume that revenue raised overseas is going to support defense-related or proliferation-linked projects.[110]

These willful violations arise in part because countries like Ethiopia find North Korea to be a reliable, low-cost partner, particularly in the defense sector.

Since the release of FATF's Mutual Evaluation Review of Ethiopia in 2015, that country remains on FATF's list of jurisdictions with strategic deficiencies.[111] While Ethiopia made a commitment to work with FATF, it has yet to establish or implement any targeted financial sanctions related to the financing of proliferation programs. However, the calculation behind Ethiopia's relations with North Korea is changing slowly. It has responded to the increased United Nations action by closing the bank accounts of many North Korean diplomats.[112] The United States can reinforce this strengthening of will through its leadership at FATF, as well as bilaterally by discussing with Addis Ababa technical deficiencies.

Case Study: Letting Pakistan off the Hook on Proliferation Finance

Several countries, including Pakistan, often slip under the radar of international efforts to find and halt proliferation finance. This is primarily because they are not currently subject to multilateral or even unilateral sanctions programs. The situation is ironic, given that Pakistan's A. Q. Khan helped create Pakistan's nuclear program and subsequently an entire network. This network spanned the United Kingdom, the Netherlands, Italy, Spain, Switzerland, Turkey, South Africa, the United Arab Emirates, Malaysia, Singapore, and South Korea, and supplied countries such as Iran, North Korea, and Libya with the parts and know-how needed to create domestic nuclear weapons programs. A decade and a half after A. Q. Khan confessed to illegally proliferating nuclear technology, Pakistani proliferation networks still operate. In 2014, the United States charged three individuals and two corporations with smuggling dual-use technologies to the Pakistan Atomic Energy Commission, which is an arm of the Pakistani military.[113]

In 2010, two other individuals in the United States were charged with exporting dual-use technology that could be used in nuclear weapons technology, including dosimeters, nuclear grade resins, and series 20M selector switches.[114] The technology eventually ended up in the hands of Pakistan's Space and Upper Atmosphere Research Commission, the Pakistan Atomic Energy Commission, Chashma Nuclear Power Plant, and the Pakistan Institute of Engineering and Applied Sciences, all entities instrumental to Pakistan's development of nuclear weapons.

Because Pakistan is not linked to a major country sanctions program, the international community and domestic political actors commonly overlook these transactions, due to a lack of political will and a lack of practical controls or a larger proliferation finance detection network. In 1979, President Jimmy Carter cut off all economic and military aid to Pakistan because of the development of nuclear weapons, using Section 101 of the Arms Export Control Act, which prohibits the United States from giving economic and military assistance to any country that the president determines is delivering or receiving nuclear equipment, materials, or technology.[115] However, in order to support the guerrillas in the Soviet-Afghan War, Carter lifted the sanctions, allowing Pakistan to expand its nuclear capabilities.

More recently, 11 days after 9/11, President George W. Bush officially lifted the sanctions that were reimposed on Pakistan after its 1998 nuclear test, in order "to cooperate more easily with Pakistan in the fight against terrorism."[116] Other outside actors such as China also help reduce the incentives for Pakistan to better implement its own illicit financing laws. On June 28, 2018, Pakistan was put back on FATF's list of jurisdictions

Pakistan's A. Q. Khan helped create Pakistan's nuclear program and subsequently an entire network.

Members of Pakistan's Ministry of Defense and high-level military officials reveal a Pakistan-made, short-range, nuclear-capable missile. Pakistan's A. Q. Khan not only helped create that country's nuclear program, he also supplied countries including Iran, North Korea, and Libya with the parts and know-how to create domestic nuclear weapons programs. (Pakistan Ministry of Defense/Getty Images)

with strategic deficiencies, which makes it harder for that country to borrow money from others to pay back its debt and deters other countries and international companies from investing in Pakistan.[117] While China did not oppose the motions to put Pakistan back on the list, two days after FATF's announcement, China gave Pakistan a $1 billion loan to help boost its foreign currency reserves.[118] Since then, the U.S. Department of State has said that Pakistan's implementation of terrorist financing through its Anti-terrorism Act of 1997 remains uneven, and the FATF assessment delegation is reportedly unimpressed with Pakistan's progress.[119]

Both international and domestic actors also seem to look past proliferation finance as long as nuclear weapons do not fall into the hands of terrorists. A. Q. Khan was forced to confess on live television in 2004 to finance proliferation, yet is now a free citizen protected by the Pakistani government from being questioned by foreign investigators. He was allowed to recant his confession and is widely known as the "Mohsin e-Pakistan," the savior of Pakistan.[120]

Resolution 1540 (2004), intended to keep WMD and their means of delivery out of the hands of non-state actors, was adopted unanimously by the Security Council in the aftermath of the A. Q. Khan affair. But the resolution focuses on equipment and materials, and requirements related to financing are relatively few. The resolution nevertheless underpins the current international countering proliferation financial regime framework, in its nascent form. But this framework, which includes U.N. sanctions on DPRK and Iran, largely misses Pakistan, as well as other major nuclear-enrichment programs in countries not targeted by the United States with high-priority diplomatic and economic measures, such as Iran and North Korea. Independent organizations, for example the Arms Control Association, say that Pakistan is "expanding its nuclear arsenal faster than any other country," yet it has largely avoided international pressure on nuclear proliferation.[121] Despite this assessment, not only has Pakistan avoided scrutiny from the United Nations, it now offers help to others under the

Both international and domestic actors also seem to look past proliferation finance as long as nuclear weapons do not fall into the hands of terrorists.

International Atomic Energy Agency's (IAEA) Technical Assistance and Technical Cooperation programs.[122] The only way that the international community can pressure Pakistan's, India's, or Syria's WMD programs is by unilateral sanctions (in the case of Syria) or export controls (for Pakistan and to a lesser extent India).

The case studies of the United States, China, Ethiopia, and Pakistan demonstrate that the problem of proliferation finance, particularly how political will undermines more aggressive action, impacts developed and developing countries alike, and countries with both weak and strong legal infrastructures. Having identified the scale and scope of the problem, the next section offers a roadmap for policymakers to address deficiencies in countering proliferation finance.

What Do We Do About It? Policy Recommendations

There are no insurmountable obstacles facing the United States in its efforts to lead on strengthening the countering proliferation finance regime. Both Congress and the executive branch broadly agree on the extent to which countering weapons of mass destruction proliferation fits into wider U.S. national security priorities. They also both see a high degree of utility in using financial measures as tools of coercion against U.S. adversaries, as evidenced by the bipartisan consensus on the use of targeted financial sanctions. The United States and its partners have compelling reasons for strengthening the focus of countering proliferation finance work. Additional steps they can take include extending regulatory controls to industries such as shipping and insurance, or grappling with the impact that new technology (virtual currency, machine learning) will have on financial crimes compliance. These steps require additional resources – often a barrier to adoption – but the short- and long-term benefits of aggressive action far outweigh the immediate costs.

More aggressive U.S. leadership is important to strengthening the regime for several reasons. The first is that the U.S. dollar is still the preferred currency for international trade, and the U.S. financial sector is still an attractive partner for international businesses. This is because of its mature equity and debt markets, the easy convertibility of the U.S. dollar, and the strong and relatively predictable nature of its legal and regulatory system. As a result, international private sector firms are highly disincentivized to run afoul of U.S. law enforcement and regulators.

Second, U.S. law enforcement and regulators are very well resourced and invested in providing technical assistance to U.S. partners where appropriate. The United States can work directly to improve the global nonproliferation regime at a time when it is involved in controversial and high-stakes diplomatic engagement surrounding Iran's and North Korea's nuclear capabilities.

A third reason for the United States to take a strong lead on countering proliferation finance is that even if other countries do not welcome U.S. leadership in this space, the United States is nevertheless uniquely well placed to apply pressure to comply with international obligations and to offer support in doing so. The resources and operational capacity of the United States can compel others to lead politically, and the pressure of running afoul of U.S. authorities can change the calculus for other countries, convincing them that fighting proliferation networks is in their national interest. The U.S. administration has used this leverage in other instances, as well as its considerable technical assistance resources, and this outlook should be developed further in the proliferation space.

The following policy recommendations outline steps that the U.S. government and the private sector can take to address the political will and prioritization needed to better recognize and combat proliferation finance. These recommendations also account for the capacity challenges laid out in this paper. Adopting these measures in part or in whole will put the United States in a much stronger position of leadership to advance the global counterproliferation community and national security for the United States and its allies.

Raise Awareness, Educate

The basic building block of a strong countering proliferation finance regime is ensuring that all relevant stakeholders are aware of what it is, why it presents such a dire risk to international peace and security, and what policies private and public sector actors can be taking to address it.

1. The Trump administration should raise awareness of and expand the expertise of the U.S. policy and intelligence community in countering proliferation finance. To that end, the president should direct the creation and publication (in unclassified form) of a U.S. National Intelligence Estimate (NIE) on proliferation finance. Such an NIE will draw widespread attention to the complex nature of the threat and underscore how different state actors, for example North Korea, Iran, and Syria, often collaborate to spread goods and know-how to advance weapons of mass destruction programs.
2. As part of that awareness raising and education effort, FinCEN should regularly release public and private advisories on proliferation finance typologies so that international financial institutions understand how these networks change their operations over time.
3. The Treasury Department should emphasize in any future guidance on proliferation finance that a rules-based, list-checking, sanctions-only approach is inadequate. Despite progress to date, far too many financial jurisdictions and institutions around the world still consider themselves in fulfillment of their regulatory obligations by taking a rules-based approach to countering illicit finance, including

proliferation finance. Foreign policy leaders and international financial institutions pay attention to statements from the U.S. Treasury Department, and they will note the emphasis on a more intensive risk-based approach to countering the financing of proliferation. U.S. banks should similarly ensure that their overseas respondents are adopting such policies toward proliferation finance.

4. The administration, particularly the Treasury Department, should partner with outside groups, and further refine its approach to public-private partnerships in order to raise awareness and further expand information-sharing efforts. A strong and growing open-source community is building knowledge about proliferation finance. Many private institutions, including think tanks, academia, and for-profit analytical firms, understand and support using financial and economic policy and tools for analysis and policy advancement on counterproliferation issues. The Trump administration can buttress these efforts by identifying opportunities to expand public-private partnerships. The Treasury Department, including FinCEN, should consider convening a formal outside advisory group to explore additional strategies for improving information sharing. These efforts could include strategies to gather and share data relevant to civil asset forfeiture, 314(b) information sharing between financial institutions, and data from demand letters. Legislation is currently pending in the U.S. House of Representatives that would provide safe harbor for nonprofit organizations to share information with financial institutions on activities potentially indicative of money laundering and human trafficking.[123] This could serve as a model for information sharing on proliferation finance for non-bank commercial institutions such as shipping, manufacturers, and freight forwarders.
5. In addition to the open-source analytical community, the administration should enhance public understanding of the proliferation threat and the importance of countering its financing. Greater discourse and outreach to explain the issue will help to dispel notions of proliferation finance being an issue for "experts" that is of significance to few. In addition, public funding to journalism on proliferation finance for "follow the money" press work would support the kind of difficult, long-term investigations that can focus attention on the seriousness of the threat. Such support will raise awareness and help to bring this into wider public consciousness, which in turn will lead to the political will for more aggressive action. Also, it will educate the frontline bank supervisors who often rely on their news consumption to understand some of the common money laundering and financial crime threats.

Change Policy at Home

While the United States sits at the center of the international financial system, its leadership is weakened by the gaps that regulators permit in financial oversight. The relative openness of the U.S. financial sector is a source of economic strength, but it should not obscure the grave difficulties that these gaps present to countering proliferation finance. To reduce the vulnerabilities in the U.S. financial sector, the administration and Congress should do the following to specifically adapt domestic law and regulation:

1. Congress should pass legislation requiring the reporting to law enforcement of the ultimate beneficial ownership of corporate entities that are created in the United States. Doing so would provide an invaluable tool for information gathering about illicit financial actors, including proliferation networks. The existing Customer Due Diligence Rule is insufficient because it only requires certain financial institutions to collect such information, without a mandate that it be automatically transmitted to government authorities. Bills such as the Corporate Transparency Act of 2017, introduced in both the House and the Senate, and the True Incorporation Transparency for Law Enforcement Act (TITLE Act), introduced in the Senate, are examples of legislation that would establish legal requirements for accurate disclosure of beneficial owners of corporate entities. Congress must lead on this, first by passing such legislation and then by using its oversight authority to spur effective implementation by the executive branch.
2. The administration should proceed with the implementation of the Customer Due Diligence Requirements for Financial Institutions Rule, which became effective in May 2018. The rule strengthens the requirement for financial institutions to verify the identity of account holders. It requires the ongoing monitoring of customer accounts for suspicious transactions. Congress should use its oversight powers to ensure that the rule implementation proceeds broadly and expeditiously.
3. Congress should consider advancing a financial requirement to mandate the declaration of all

cross-border payments, possibly including information that would be relevant to bridging the gap between data about financial transactions and the physical shipment of potentially proliferation-related goods. As currently formulated, the Travel Rule is only for transactions above $3,000 and requires only retention, not transmittal to relevant authorities. Congress and the administration should consider the categories of information that would be feasible to incorporate in such a cross-border rule, including beneficial ownership, underlying goods, transaction participants, industry of senders and beneficiaries, and transparency about the final destination of goods for trade-specific transactions. U.S. partners Canada and Australia already operate significantly tougher Cross-Border Transfer Rules.

4. U.S. law enforcement agencies should expand their work on information sharing and public-private partnerships. This could be led by the weapons of mass destruction directorate at the FBI and Department of Homeland Security (DHS) investigations, as both agencies have taken the lead on evidence collection for past WMD proliferation prosecutions. The FBI director and the DHS secretary should make this a priority for their respective agencies. They should explore the creation of an external advisory group to pilot information sharing and, working with the Treasury Department and relevant financial regulators, safe harbor mechanisms. This effort should include shippers and manufacturers as well.
5. Executive agencies and financial regulators should explore regulatory carve-outs for innovations on countering proliferation finance. These innovations could include:
   - » Major U.S. banks (and others that participate in dollar clearing through their correspondent banking relationships) investing in big data approaches to transaction monitoring and aggregating trade and financial data.
   - » The federal banking agencies and state banking licensing authorities should give special recognition and dispensation to banks to train their correspondent institutions on using data to collect information on suspected proliferation finance activity.
   - » The corresponding federal and state financial institution supervisory authorities should structure their exams so that financial activity that may be national security–sensitive is treated differently
   - » The Financial Crimes Enforcement Network could create a dedicated supervisory team to examine for proliferation financing risk, as has been recommended previously by banking policy organizations such as the Clearing House.
6. Congress should prioritize additional funding increases on a yearly basis for the Treasury Department's Office of Terrorism and Financial Intelligence (TFI) in order to more adequately, and on an ongoing basis, provide resources for activities to counter proliferation finance. TFI is at the front line of policy innovation on countering proliferation finance. Its activities include the formulation and enforcement of all financial measures to counter weapons of mass destruction. Congress recently increased TFI funding, but the appropriation was less than what the Treasury Department had originally requested.
7. The Treasury Department should convene an interagency process to consider the development of new regulations that would require U.S. banks and the shipping, freight forwarding, and manufacturing sectors to collaboratively gather more information on the parties to, and purpose of, proliferation activities. The United States should furthermore initiate a formal process with international counterparts to push for complementary, joint compliance efforts abroad.

The Financial Crimes Enforcement Network, whose director, Kenneth A. Blanco, is pictured here, could work with other U.S. law enforcement agencies to help combat proliferation financing through expanding information sharing and private-public partnerships. (Justin Sullivan/Getty Images)

8. FinCEN should dedicate intensive efforts to analyze SARs for proliferation finance activities and develop refined indicators and explore opportunities for greater proactive sharing of relevant information with other proliferation-related U.S. government agencies and banks. When shared with the private sector, this information may lead to the most fruitful investigation and analysis of proliferation networks and the filing of so-called super-SARs that may be highly advantageous to law enforcement efforts.

Lead Abroad

The United States has opportunities in both its bilateral and multilateral interactions to improve the global countering proliferation finance regime. U.S. government action is necessary to push these countries to accept a broader approach, given U.S. capacity and resources, as well as the economic and political impediments that prevent many foreign countries from undertaking concerted efforts to counter proliferation finance.

1. The Treasury Department, U.S. law enforcement agencies, and the intelligence community should launch a formal process to work with European Union jurisdictions to more formally align intelligence collection requirements, intelligence exchange, and information sharing on proliferation finance. Because proliferation finance networks desire high-quality goods for their weapons of mass destruction program, they prefer manufacturers from the United States and Western Europe, as evidenced by the purchase trail of prior procurement networks.[124] As a result, transatlantic coordination on countering proliferation finance must be a cornerstone of the wider regime. The administration should focus on identifying ideas for coping with legal and privacy impediments between the jurisdictions that have, in the past, been an obstacle to more aggressive action. While multilateral coordination is needed, the United States should be prepared to do more on its own, and with its own private sector, if the wider international community moves too slowly. This process should explore the possibility of a regulatory carve-out under the General Data Protection Regulation for anti–money laundering and proliferation finance information sharing.
2. The administration, with the Department of the Treasury in the lead, should model a proliferation finance threat cell on other financial crimes compliance data-sharing mechanisms. This could be created either as a U.S.-only or a multilateral data-sharing exercise.
3. The U.S. Treasury Department should continue to prioritize proliferation finance as part of its working agenda for its presidency of FATF. The current U.S. agenda at FATF emphasizes criminalization, expanded use of targeted financial sanctions by national authorities, and the weakness of the FATF standards for proliferation financing as compared with money laundering and terrorist financing. The United States delegation should support this work, as well as efforts by FATF to conceive of ways to gauge the feasibility of expanding this work so that it includes the following measures: encouraging the use of proliferation finance specific risk assessments, adding proliferation finance formally into the recommendations, and addressing the extent to which the shipping and insurance sectors serve as facilitators of proliferation finance. The overarching goal should be to bring FATF's approach on countering proliferation finance to the strength that both it and the United Nations demonstrate on countering terrorist financing. This should include ensuring that all nations are evaluated on the full suite of UNSCR 1540 financial requirements. The United States should ask FATF to prepare interpretive notes on United Nations obligations, including guidance on implementation of financial provisions of Resolution 1540.
4. The U.S. Treasury Department should encourage further cooperation between the high-risk jurisdictions of Hong Kong and Singapore. Both are at the front lines of proliferation finance concerns, particularly as related to North Korean networks. The United States could launch a pilot partnership with Hong Kong and Singapore so that, as a united effort, the jurisdictions could put together trade and financial data to understand the full breadth of proliferation threats and risks. These foreign jurisdictions are aware of their vulnerabilities, but they face restrictions due to legal barriers and other political and economic priorities. Such work could lead to the issuance of a series of public circulars and private advisories to banks about risks, which would help private sector actors in both jurisdictions who were eager to comply with the obligations.
5. The United States should lead the international community to develop a convention on countering proliferation finance, similar to the one that currently exists for countering terrorist financing. There are numerous opportunities for pushing for a multilateral consensus:

- » Leverage the United Nations 1540 Committee expertise on countering weapons of mass destruction proliferation to focus on member states' performance on combating proliferation finance. UNSCR 1540 places very specific obligations on member states to place effective controls to prevent the proliferation of weapons of mass destruction, including on financing, but their work program to date has not included significant efforts against proliferation finance.
- » Convene a major gathering of Group of 20 (G-20) finance ministers to address this topic at a forthcoming World Bank–International Monetary Fund meeting.
- » Convene a major gathering of foreign ministers on the sidelines of the United Nations General Assembly to discuss how to augment capabilities and technical assistance globally.
- » Put pressure on the Egmont Group, the global network of financial intelligence units, to enhance information sharing relevant to proliferation finance. These measures could include more detailed public and private advisories on proliferation finance typologies. The Egmont Group could create new information sharing mechanisms that do not violate individual member state privacy laws.

World Bank President Jim Yong Kim listens to reporters' questions during a news conference at the IMF. Leading multilateral financial institutions such as the World Bank and the International Monetary Fund could play a role in helping to develop an international convention on countering proliferation finance. (Chip Somodevilla/ Getty Images)

6. The U.S. Treasury and Commerce Departments should cooperate to identify which obstacles are preventing the extension to other industries and sectors in the global supply chain a consistent system of controls and regulations for countering proliferation finance. Other regulatory regimes that need to be built or strengthened include those in shipping, insurance, transhippers, and other nodes in the global supply chain. For the shipping industry in particular, there should be a requirement for the International Maritime Organization unique identifier numbers of ships to be added to bills of lading in trade transactions. Proliferation networks, particularly North Korean ones, have been adept at changing ship names after the vessels have been designated to evade scrutiny. The U.S. Treasury and Commerce Departments, in partnership with international regulators, should require that companies tracking ship transponders to immediately notify relevant authorities when those transponders are turned off mid-voyage. The incidences of transponder shut-off should inform private advisories to banks to flag which trading companies are utilizing vessels which are habitually tampering with transponder tracking.
7. The United States should work with counterpart governments to anonymize trade control violation data to issue joint advisories on proliferation threats. For example, the U.S.-U.K. Financial Regulatory Working Group, which seeks ways to deepen regulatory cooperation between the two countries, could issue joint recommendations on how to counter proliferation finance. The United States and the European Union also have a Joint Financial Regulatory Forum that regularly exchanges views on relevant developments. Both are models for developing fora to discuss emerging regulatory challenges. Regulators and law enforcement must enable global firms to link trade control violations to financial data, which are difficult for international banks to see on their own. Doing so can help motivate more data gathering, analysis, and operational activity on countering proliferation finance. Widening the aperture beyond attention to international banks can encourage an all-of-government effort to attack proliferation finance.
8. The U.S. administration should ask Congress for more resources to expand technical assistance programs run by the Departments of State (Export Control and Related Border

Security – EXBS – or the Bureau of International Security and Nonproliferation) and Defense (Defense Threat Reduction Agency). These programs enable partner countries to tighten their regulatory and legal regimes to combat proliferation finance. Their efforts are supported by a global network of FBI and Drug Enforcement Agency legal attachés serving in U.S. embassies throughout the world. Congress should provide additional targeted funding so that the administration can prioritize assistance to high-risk jurisdictions. Technical assistance should include efforts to share model laws from other jurisdictions. EXBS should be given funds to hold training overseas on countering proliferation finance. Coordination of outreach abroad is needed to ensure priorities are aligned and gaps filled.

9. Congress is currently taking steps to require the administration to create a Virtual Currency Task Force. If that is accomplished, the administration should instruct it to produce analysis on the impact of financial technology on financial crimes compliance, including its specific application to countering proliferation finance. If financial technology innovations circumvent those pathways, a countering proliferation finance regime will be harder to uphold.
10. The U.S. Treasury and its counterpart finance ministries in the European Union could explore the feasibility of expanding the amount of payment information that can be included in SWIFT messages. Current SWIFT messages do not allow for enough information to be conveyed about the underlying purpose of the transaction. Expanding the character limit for SWIFT messages, and requiring specific disclosures of the "who" and "why" of the transaction, would provide banks and law enforcement/intelligence agencies with more information about potential proliferation activity.

Challenge Specific State Actors

In addition to the United States leading on strengthening the global regime, it should pay special attention to the intersection between proliferation finance issues and the U.S. approach to Iran and North Korea:

1. In denuclearization talks with North Korea, the United States should outline how Pyongyang's dedication to financial transparency and cessation of proliferation finance activities must be part of any sanctions-rollback framework. Additionally, the United States should take steps to address the issues that have put North Korea on FATF's black list. Ensuring that Pyongyang disassembles the proliferation networks that procured its weapons of mass destruction program will be an important confidence-building measure. It will be necessary for the administration to feel that it is depriving North Korea of a dangerous capability. Abandoning its proliferation finance activities will be the only way for the Kim regime to facilitate a credible reentry into the global economy, legitimizing much of China's trade with Pyongyang. If North Korea fails do so, it will face very difficult reputational risks, freezing reinvestment and setting it into a more adversarial relationship with the United States. The latter could encourage North Korea to submit a first report on implementation of Resolution 1540 (2004). North Korea is the most significant of 12 or so countries that have yet to submit a report.
2. Mindful of the differences in international approaches to Iran policy, the United States should work constructively with its partners on curtailing covert Iranian proliferation activities, which are a threat to the wider international community. The international community still maintains a broad consensus against Iran obtaining advanced nuclear capabilities. As concerns grow that a potential Iranian exit from the JCPOA will raise the proliferation risk emanating from that country, so too do specific fears about it operationalizing prior

South Koreans watch U.S. President Trump meet with North Korean leader Kim Jong-un during the historic Singapore Summit. During its denuclearization talks with North Korea, the United States should ensure that the country disassembles the proliferation networks that enable its WMD program. (Chung Sung-Jun/Getty Images)

proliferation networks, including sophisticated financial channels. The U.S. return to a maximum pressure campaign will include a comprehensive targeting of Iran's financial system. But should the United States not work on this with its partners, the JCPOA framework for inspection and verification will be undermined and political relations among the parties will be frayed. The U.S. government can build on FinCEN's October 11, 2018, advisory by regularly releasing advisories on Iranian proliferation finance concerns. Mindful of the major political disagreements among transatlantic allies about how to approach Iran issues, focusing on a CPF workstream may keep collaborators focused on common concerns.

Lead in the Private Sector

Because private sector actors, especially financial institutions, sit at the front lines of countering proliferation finance, it is essential that they invest in building their subject matter expertise on this important issue. Support from national authorities, including information on specific threats, is essential. Those efforts must be joined up with aggressive private sector action:

1. The private sector has an essential role to play in implementing anti–proliferation finance measures and in collaborating on monitoring critical threats. Sophisticated private sector actors, such as major global banks, should consider collaborative analytics that bring together the results from transaction monitoring of networks from high-risk state actors, for example North Korea and Iran. The results of this analytical work should be published, building on examples provided by some global banks at professional gatherings, including Association of Certified Anti–Money Laundering Specialists (ACAMS) meetings.[125] High-risk but sophisticated jurisdictions, such as Singapore and Hong Kong, can lead in this effort. Existing models for this type of work include the way U.K. Finance and the Consortium, venues for private sector information sharing in the United Kingdom and the United States respectively, provide a forum for discussion of experiences and research on typologies and red flags. There would be no practical obstacle to substantive work on transaction monitoring strategies.
2. The private sector, especially banks with significant experience and expertise, should lead in making the most of existing information-sharing mechanisms, for example the Joint Anti–Money Laundering Intelligence Task Force (JMLIT) in the United Kingdom and the Consortium in the United States, to focus specifically on proliferation finance cases. For both JMLIT and the Consortium, proliferation finance is only one of an entire category of financial crimes issues considered, and many members fall into the trap of considering countering proliferation finance to be the concern of sanctions compliance or export control, rather than a unique challenge requiring more policy creativity.
3. The private sector should be proactive in compiling and sharing proliferation finance typologies, recognizing that there is substantial value in aggressive responses to serious national security threats. Such action offers significant reputational benefits. Private sector actors have been successful at identifying nodes of those networks through investigations within their own business operations. These firms do not have many opportunities to share relevant information about their discoveries. Doing so can avoid many privacy and information-sharing hurdles in the short term, as information about specific customers and companies can be safely anonymized and released publicly.

Conclusion

Preventing the spread of weapons of mass destruction is an essential priority for the international community. Despite this, gaps in the countering proliferation finance regime exist at the multilateral and national level. Some of these are political; others are related to capacity and resources. Regardless of the source of the deficiency, it is essential for the world to get this issue right.

While filling in and strengthening the global legal and regulatory framework is a critical step, it is ultimately dependent on the exercise of political will. If years of grave conversation about nuclear threats at the United Nations, and the erosion of core arms control regimes, have not motivated political will, then the United States should take more aggressive leadership to push forward international laws and obligations on countering proliferation finance. Repeatedly, governmental officials, bank executives, and independent observers privately note that to overcome competing economic and political

The advances in financial technology are causing major financial and transshipment hubs to understand how to regulate virtual currencies such as Bitcoin. It is highly likely that proliferation networks will try to exploit cryptocurrencies and other new financial technologies to continue their illicit activities. (Dan Kitwood/Getty Images)

interests that serve to undermine true efforts to expose and halt proliferation finance, powerful legal compulsion or significant reputational risk will be required. The United States is unique in its capability to deliver this kind of change and thereby enable a change in political will. The Trump administration has emphasized, in its strategic approach to adversaries Iran and North Korea, that it is concerned about the proliferation of weapons of mass destruction. It has used diplomatic and economic tools to constrain the ability of both countries to expand their arsenal (especially in the case of North Korea) and return to an enrichment path that could include a weaponization component (in the case particularly of Iran).

The United States has a window to lead multilaterally at the United Nations and FATF, bilaterally in its diplomatic relationship with important financial jurisdictions, and nationally with its own laws, regulations, and procedures. The layers of cooperation required will

The initial steps to counter WMD proliferation must be taken now, before the international community deals with a paradigm-shifting event.

be built over the long term, but the initial steps must be taken now, before the international community deals with a paradigm-shifting event. If a U.S. adversary gains a permanent nuclear or other WMD capability and uses it during a crisis, the policy response will be much more overwhelming and restrictive than preventative measures that can be taken now to redress the gaps in the regulatory regime.

This urgency is underscored by the fact that the nature of the threat is continuously evolving. During the past few years, North Korea has demonstrated its sophisticated cyberspace capabilities. Recent reporting has identified new typologies showing that North Koreans are raising money through social media and mobile application software (apps) tied to the gig economy.[126] The U.S. Treasury Department has responded with sanctions targeting information technology firms in China and Russia, but, as this report has demonstrated, sanctions enforcement alone is insufficient to counter this threat.[127]

This is particularly true given the pace of technological change, particularly in the financial technology space. Virtual currency, distributed ledger technology, and the application of artificial intelligence to amassing and analyzing data all promise to remake how consumers and institutions interact with the global financial system. Jurisdictions are trying to understand how to regulate virtual currencies such as Bitcoin.[128] Several major financial and transshipment hubs are also working to understand how new technology is impacting the architecture of global trade.[129] International banks already have problems in matching trade data with

financial data, a situation that proliferation networks have exploited to obscure the illicit acquisition of WMD goods within the wider sphere of global trade. New data solutions, including artificial intelligence, may enable faster and more systematic analysis of this data, enabling banks to have significantly more visibility. While the exact course of those developments is hard to predict, because existing proliferation finance networks and methodologies are neutralized by actions of the international community, it is highly likely that proliferation networks will try to exploit new technology to continue their illicit activities. Regulators at both the international and national levels have an important role to play in advancing rules to leverage new technology solutions – and the time to do so is now.

Identification of proliferation financing offers the international community an additional tool to recognize emerging WMD proliferation networks. Effectively combating proliferation financing will not by itself stop this proliferation, but it is a tool with huge potential, particularly if deployed cross-jurisdictionally. The international community needs to grasp these tools now. Ultimately, U.S. leadership has a critical role to play in the process. The next few years will determine whether the gaps in the regime can be patched to the extent required to push back on the WMD threat from U.S. adversaries.

Endnotes

1. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, S/2014/147 (March 6, 2014), http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/147.

2 According to FATF, the definition of proliferation finance refers to "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."

3. See, for example, adaptations in the use of export of coal through shipping networks. Joby Warrick, "High Seas Shell Game: How a North Korean Shipping Ruse Makes a Mockery of Sanctions," *The Washington Post*, March 3, 2018, https://www.washingtonpost.com/world/national-security/high-seas-shell-game-how-a-north-korean-shipping-ruse-makes-a-mockery-of-sanctions/2018/03/03/3380e1ec-1cb8-11e8-b2d9-08e748f892c0_story.html?utm_term=.71827c1f301f.

4. See Case Study 19 in Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation," Final Report (King's College London, October 2017), https://projectalpha.eu/wp-content/uploads/sites/21/2018/05/FoP-13-October-2017-Final.pdf.

5. Press coverage of the as-yet unreleased United Nations Panel of Experts report indicates that the U.N. experts have concluded that North Korea's networks "operate with little or no constraints in five main countries." Colum Lynch, "U.N. Report Details How North Korea Evades Sanctions," *Foreign Policy*, September 20, 2018, https://foreignpolicy.com/2018/09/20/un-report-details-how-north-korea-evades-sanctions/.

6. On enforcement actions, see the imposition of Patriot Act 311 measures against the China-based Bank of Dandong for "serving as a conduit" between North Korea and the international financial system, to the direct benefit of North Korea's nuclear program. Department of the Treasury, Financial Crimes Enforcement Network, "Imposition of Special Measure Against Bank of Dandong as a Financial Institution of Primary Money Laundering Concern," Federal Register 82, no. 215 (November 8, 2017): 51758, https://www.fincen.gov/sites/default/files/federal_register_notices/2017-11-08/Dandong%20Final%202017-24238.pdf. The U.S. objectives for its FATF presidency can be found at: "Objectives for FATF — XXX (2018-2019)," Financial Action Task Force, June 29, 2018, http://www.fatf-gafi.org/media/fatf/content/images/Objectives%20for%20FATF-XXX%20(2018-2019).pdf.

7. Richard A. Clarke, "Statement of Richard A. Clarke," Testimony before the U.S. Senate Banking Committee, October 22, 2003, https://www.banking.senate.gov/imo/media/doc/clarke.pdf.

8. "Bin Laden Papers Including Loving Notes, Terrorist Application," *Chicago Tribune*, May 20, 2015, http://www.chicagotribune.com/news/nationworld/ct-osama-bin-laden-documents-20150520-story.html.

9. Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs, 2013).

10. "Global Terrorism in 2017," START Background Report (University of Maryland, August 2018), https://www.start.umd.edu/pubs/START_GTD_Overview2017_July2018.pdf.

11. Thomas Renard, "Europe's 'New' Jihad: Homegrown, Leaderless, Virtual," Security Policy Brief No. 89 (Egmont Institute, July 2017), http://www.egmontinstitute.be/content/uploads/2017/07/89.spb_.amended.pdf?type=pdf.

12. United Nations 1540 Committee, "Message from the 1540 Committee Chair" (November 2018, issue 15), http://www.un.org/en/sc/1540/chair-message.shtml.

13. William B. Messmer and Carlos L. Yordán, "A Partnership to Counter International Terrorism: The U.N. Security Council and the U.N. Member States," *Studies in Conflict & Terrorism* 34 no. 11 (October 2011), http://www.tandfonline.com/doi/full/10.1080/1057610X.2011.611932?src=recsys.

14. United Nations Counter-Terrorism Committee, *Global Survey of the Implementation of Security Council Resolution 1373 (2001) by Member States*, S/2011/463 (September 1, 2011), 6, https://www.un.org/sc/ctc/wp-content/uploads/2016/01/2011-globalsurvey1373.pdf.

15. United Nations General Assembly, *International Convention for the Suppression of the Financing of Terrorism,* Resolution 54/109 (December 9, 1999), http://www.un.org/law/cod/finterr.htm.

16. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, S/2018/171 (February 1, 2018), http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171.

17. Michelle Nichols, "U.N. to Vote on New North Korea Sanctions on Monday Afternoon: Diplomats," Reuters, September 10, 2017, https://www.reuters.com/article/us-northkorea-missiles-un/u-n-to-vote-on-new-north-korea-sanctions-on-monday-afternoon-diplomats-idUSKCN1BM06W.

18. Barry Hart Dubner and Mary Carmen Arias, "Under International Law, Must a Ship on the High Seas Fly the Flag of a State in Order to Avoid Being a Stateless Vessel? Is a Flag Painted on Either Side of the Ship Sufficient to Identify It?," Digital Commons @ Barry Law, 29 U.S.F.

Mar. L. J. 99 (2017), https://lawpublications.barry.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1120&context=facultyscholarship.

19. Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (February 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

20. Financial Action Task Force, *FATF Guidance on Counter Proliferation Finance: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction* (February 2018), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf.

21. United Nations Security Council, *Letter from the Chair of the Security Council Committee Established Pursuant to Resolution 1540 (2004)*, S/2016/1038 (9 December 2016,), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/1038.

22. Authors' interviews with bank officials in Singapore and Hong Kong.

23. Kenneth A. Blanco, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, "S. 1241: Modernizing AML Laws to Combat Money Laundering and Terrorist Financing," Statement to the Committee on the Judiciary, U. S. Senate, November 28, 2017, https://www.judiciary.senate.gov/imo/media/doc/Blanco%20Testimony.pdf.

24. Jonathan Stempel, "U.S. Seeks Funds Tied to North Korea from Eight Big Banks," Reuters World News, July 6, 2017, https://www.reuters.com/article/us-usa-northkorea-banks-idUSKBN19S014.

25. "Taiwan Businessman Sentenced to 24 Months for Conspiring to Violate U.S. Laws Preventing Proliferation of Weapons of Mass Destruction," U. S. Department of Justice, press release, March 16, 2015, https://www.justice.gov/opa/pr/taiwan-businessman-sentenced-24-months-conspiring-violate-us-laws-preventing-proliferation.

26. Bureau of Industry and Security, *Export Administration Regulations: General Regulations*, Part 736 (March 16, 2016), https://www.bis.doc.gov/index.php/documents/regulation-docs/413-part-736-general-prohibitions/file.

27. Bureau of Industry and Security, *Control Policy: End-User and End-Use Base*, Part 744 (June 6, 2018), https://www.bis.doc.gov/index.php/documents/regulation-docs/418-part-744-control-policy-end-user-and-end-use-based/file.

28. Ibid.

29. Authors' interview with European bank official.

30. "Trade Finance Principles" (Wolfsberg Group, International Chamber of Commerce, and BAFT, 2017), 7, http://www.baft.org/docs/default-source/policy-department-documents/final-clean-trade-finance-principles-final.pdf?sfvrsn=2.

31. "Trade Finance Principles" (Wolfsberg Group, ICC, and BAFT, 2017), 19, https://cdn.iccwbo.org/content/uploads/sites/3/2017/01/ICC-Wolfsberg-Trade-Finance-Principless-2017.pdf.

32. Elizabeth Rosenberg, Senior Fellow and Director of the Energy, Economics, and Security Program, Center for a New American Security, "Countering the Financial Networks of Weapons Proliferation," Testimony to the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, July 12, 2018, https://www.cnas.org/publications/congressional-testimony/testimony-before-the-house-financial-services-committee-subcommittee-on-terrorism-and-illicit-finance.

33. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Update on the Continuing Illicit Finance Threat Emanating from North Korea," FinCEN Advisory FIN-2013-A005, July 1, 2013, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2013-a005.

34. Financial Action Task Force, *Anti–Money Laundering and Counter-Terrorist Financing Measures: United States: Fourth Round Mutual Evaluation Report* (December 2016), https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

35. United Nations Security Council, *Resolution 2397* (2017), http://undocs.org/S/RES/2397(2017).

36. U. S. Department of the Treasury, *Settlement Agreement*, COMPL-2013-193659 (June 30, 2014), https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140630_bnp_settlement.pdf; "Treasury Department Reaches Landmark Settlement with HSBC," U.S. Department of the Treasury, press release, December 11, 2012, https://www.treasury.gov/press-center/press-releases/Pages/tg1799.aspx; U.S. Department of the Treasury, *Settlement Agreement between U.S. Department of Treasury's Office of Foreign Assets Control and Commerzbank AG*, FAC No. 713262 (March 12, 2015), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150312.aspx.

37. 18 U.S.C. § 1956, "Laundering of Monetary Instruments," https://www.law.cornell.edu/uscode/text/18/1956.

38. Sonia Ben Ouagrham-Gormley, "Banking on Nonproliferation: Improving the Implementation of Financial Sanctions," *The Nonproliferation Review* 19, no. 2 (June 2012), http://www.tandfonline.com/doi/full/10.1080/10736700.2012.690963?src=recsys#.

39. 31 CFR § 1020.220, "Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks," https://www.law.cornell.edu/cfr/text/31/1020.220.

40. Authors' interviews with U.S. government officials.

41. Authors' interviews with current and former U.S. law enforcement officials.

42. Emil Dall, Tom Keatinge, and Andrea Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions" (Royal United Services Institute [hereafter RUSI] Guidance Paper, April 2017), 12, https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf.

43. "Treasury Designates Banco Delta Asia as Primary Money Laundering Concern under USA PATRIOT Act," U.S. Department of the Treasury, press release, September 15, 2005, https://www.treasury.gov/press-center/press-releases/Pages/js2720.aspx.

44. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies," FinCEN Advisory FIN -2017-A001, January 19, 2017, https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a001.

45. "FinCEN Further Restricts North Korea's Access to the U.S. Financial System and Warns U.S. Financial Institutions of North Korean Schemes," U.S. Department of the Treasury, Financial Crimes Enforcement Network, press release, November 2, 2017, https://www.fincen.gov/news/news-releases/fincen-further-restricts-north-koreas-access-us-financial-system-and-warns-us.

46. Financial Action Task Force, *Combating Proliferation Finance: A Status Report on Policy Development and Consultation* (February 2010), http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.

47. Anagha Joshi, "Model Provisions to Combat the Financing of the Proliferation of Weapons of Mass Destruction," 2nd ed. (RUSI: July 2018), https://rusi.org/sites/default/files/20181002_model_law_2nd_edition_final_for_web.pdf.

48. European Commission, "Dual-use trade controls," May 28, 2018, http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

49. HM Treasury (United Kingdom), "HM Treasury Advisory Notice: Money Laundering and Terrorist Financing Controls in Higher Risk Jurisdictions," MLRs 2017, n.d. (2018), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664503/Money_laundering_and_terrorist_financing_controls_in_overseas_jurisdictions___advisory_notice.pdf.

50. "Proceeds of Crime Act 2002 Part 7: Money Laundering Offences," s.330, Crown Prosecution Service, https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences.

51. "Proceeds of Crime: Prevention and Suppression of Terrorism," Criminal Finances Act 2017 (Commencement No. 3) Regulations 2017, No. 1028 (C.94), http://www.legislation.gov.uk/uksi/2017/1028/pdfs/uksi_20171028_en.pdf.

52. Anti-terrorism, Crime and Security Act 2001 (C.24), https://www.legislation.gov.uk/ukpga/2001/24/contents.

53. Office of Financial Sanctions Implementation, HM Treasury, *Financial Sanctions: Guidance* (March 2018), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/645280/financial_sanctions_guidance_august_2017.pdf.

54. Michael Sharvin, "UK Government to Implement a Register of Beneficial Owners of Overseas Entities That Own UK Real Estate," Ince & Co LLP, April 24, 2018, Lexology, https://www.lexology.com/library/detail.aspx?g=7384e063-e972-4e3a-acbf-4990d71264c0.

55. Andrea Berger and Anagha Joshi, "Guidance Paper: Countering Proliferation Finance: Implementation Guide and Model Law for Governments," (RUSI, July 2017), https://rusi.org/sites/default/files/201707_rusi_cpf_implementation_guide_and_model_law_berger_joshi_0.pdf.

56. Strategic Trade Act (STA) 2010, Ministry of International Trade and Industry, http://www.miti.gov.my/index.php/pages/view/sta2010?mid=105.

57. Financial Action Task Force, *Anti–Money Laundering and Counter-Terrorist Financing Measures: Malaysia: Mutual Evaluation Report*, September 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Malaysia-2015.pdf.

58. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 2131 (2014)*, S/2015/131 (February 23, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/131.

59. Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act, B.E. 2559 (2016), http://www.amlo.go.th/amlo-intranet/media/k2/attachments/CTPF%20Act_1.pdf.

60. "High-Risk and Other Monitored Jurisdictions," Financial Action Task Force, http://www.fatf-gafi.org/countries/#high-risk.

61. "Public Statement," Financial Action Task Force, press release, June 29, 2018, http://www.fatf-gafi.org/countries/d-i/iran/documents/public-statement-june-2018.html.

62. Financial Action Task Force, *Anti–Money Laundering and Combating the Financing of Terrorism, Mutual Evaluation,*

8th Follow-up Report: China (February 17, 2012), http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Follow%20Up%20MER%20China.pdf.

63. "Improving Global AML/CFT Compliance: On-going Process – 29 June 2018," Financial Action Task Force, press release, June 29, 2018, http://www.fatf-gafi.org/countries/d-i/iraq/documents/fatf-compliance-june-2018.html.

64. "Outcomes FATF Plenary, 17–19 October 2018," Financial Action Task Force, October 19, 2018. http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html#two.

65. Ibid.

66. Andrea Berger, "A House Without Foundations: The North Korea Sanctions Regime and Its Implementation," (RUSI, June 9, 2017), https://rusi.org/publication/whitehall-reports/house-without-foundations-north-korea-sanctions-regime-and-its; Emil Dall, Tom Keatinge, and Andrea Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions" (RUSI, April 2017), https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf; and Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation" (Center for a New American Security, January 2018), among others.

67. Authors' interviews with bank executive in Hong Kong.

68. For discussions of improving guidance from regulators to financial institutions see, *inter alia*, Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation"; and Dall, Keatinge, and Berger, "Countering Proliferation Finance: An Introductory Guide."

69. Jersey Financial Services Commission, *Guidance on Proliferation and Proliferation Financing,* Jersey Financial Services Commission, October 2011; Central Bank of the Bahamas, Compliance Commission of the Bahamas, Insurance Commission of the Bahamas, and Securities Commission of the Bahamas, *Guidance Note on Proliferation and Proliferation Financing*, Central Bank of the Bahamas, Compliance Commission of the Bahamas, Insurance Commission of the Bahamas, and Securities Commission of the Bahamas, August 21, 2018.

70. Authors' interview with Western European banking regulation expert.

71. Authors' interviews with banking executives in Hong Kong, Singapore, and Malaysia.

72. The Clearing House, *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement* (February 2017), 7, The Clearing House, https://www.theclearinghouse.org/-/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.

73. David Thompson, "Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System" (C4ADS, 2017), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/59413c8bebbd1ac3194eafb1/1497447588968/Risky+Business-C4ADS.pdf.

74. Council Regulation 2016/679/EC on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), European Parliament, April 26, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679; and authors' interviews with bank officials.

75. See the text of the Final Customer Due Diligence Rule at Federal Register, U.S. Department of the Treasury, Financial Crimes Enforcement Network, *Customer Due Diligence Requirements for Financial Institutions*, 81, no. 91 (May 11, 2016), 29398-29458, https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

76. Financial Action Task Force, *Anti–Money Laundering and Counter-Terrorist Financing Measures: Mutual Evaluation Report* (December 2016), 224, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

77. "A New Standard on Beneficial Ownership: Where Do the U.S. and Canada Stand?" Transparency International, May 10, 2018, https://voices.transparency.org/a-new-standard-on-beneficial-ownership-transparency-where-do-the-us-and-canada-stand-fb8caa6bad66.

78. Nathalie Colin, Willem Van de Wiele, Alexandre Hublet, Olivier Van Wuowe, and Elien Claeys, "Adoption of Fifth Anti-Money Laundering Directive," White & Case, https://www.whitecase.com/publications/alert/adoption-fifth-anti-money-laundering-directive.

79. "Their overly broad and vague definitions, unworkable requirements, and severe penalties would do far more to impede law abiding small and medium-sized business than to hamper the use of so-called 'shell companies' to facilitate illicit activity." Brian O'Shea, Senior Director, Center for Capital Markets Competitiveness, U.S. Chamber of Commerce, "Beneficial Ownership: Fighting Illicit International Financial Networks Through Transparency," Testimony to the Senate Judiciary Committee, February 6, 2018, https://www.uschamber.com/sites/default/files/020618_brian_oshea_testimony_beneficial_ownership.pdf.

80. M. Kendall Day, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, "Beneficial Ownership: Fighting Illicit International Financial Networks through Transparency," Testimony to the Senate Judiciary Committee, February 6, 2018, https://www.judiciary.senate.gov/imo/media/doc/02-06-18%20Day%20Testimony.pdf.

81. Brewer, "Study of Typologies of Financing of WMD Proliferation."

82. Daniel Salisbury and Ian J. Stewart, "Li Fang Wei (Karl Lee)," Proliferation Case Study Series (Project Alpha, King's College, London, May 19, 2014), http://kcl-di-gi-prod-wa-wordp-ne-04.azurewebsites.net/alpha/wp-content/uploads/sites/21/2014/09/Karl-Li-case-study-final.pdf.

83. Glenn Kessler, "U.S. Links Iranian Bank to Fifth Avenue Building," *The Washington Post*, December 18, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/12/17/AR2008121703844.html.

84. Financial Action Task Force, *Anti–Money Laundering and Counter-Terrorist Financing Measures: Mutual Evaluation Report*, 224.

85. "Hearing Entitled 'Countering the Financial Networks of Weapons Proliferation,'" House Financial Services Committee, July 12, 2018, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=403709; "Hearing Entitled 'Implementation of FinCEN's Customer Due Diligence Rule – Financial Institutions Perspective,'" House Financial Services Committee, April 27, 2018, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=403343.

86. Authors' interviews with government officials.

87. Authors' interviews with government regulators and bank executives in Hong Kong, Malaysia, Singapore, and the United Kingdom.

88. Elizabeth Rosenberg, Director and Senior Fellow, Center for a New American Security, testimony to the Committee Subcommittee on Terrorism and Illicit Finance, Financial Services Committee, U.S. House of Representatives, July 12, 2018, 6, https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-erosenberg-20180712.pdf.

89. Lynch, "U.N. Report Details How North Korea Evades Sanctions."

90. Jason Arterburn, "Dispatched: Mapping Overseas Forced Labor in North Korea's Proliferation Finance System" (C4ADS, 2018), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5b631c9b2b6a2845024e4ff5/1533222111619/Dispatched+Final-2.pdf.

91. Donald J. Trump, Twitter post, July 9, 2018, 7:25 a.m., https://twitter.com/realDonaldTrump/status/1016327387154395138?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1016327387154395138&ref_url=https%3A%2F%2Fthehill.com%2Fhomenews%2Fadministration%2F396087-trump-china-may-be-exerting-negative-pressure-on-nuclear-deal-with.

92. "Treasury Imposes Sanctions on Supporters of North Korea's Weapons of Mass Destruction Proliferation," U.S. Department of the Treasury, press release, September 26, 2018, https://www.treasury.gov/press-center/press-releases/Pages/jl5059.aspx; Thompson,"Risky Business."

93. Agence France-Presse, "In China, North Korean Firms Still Trading Despite Shutdown Order," *South China Morning Post*, January 9, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2127530/china-north-korean-firms-still-trading-despite-shutdown.

94. Eleanor Albert, "The China-North Korea Relationship," CFR.org, March 28, 2018, https://www.cfr.org/backgrounder/china-north-korea-relationship.

95. "Treasury Sanctions Trading, Labor, and Shipping Companies and Vessels to Further Isolate North Korea," U.S. Department of the Treasury, press release, November 21, 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0220.aspx.

96. "2016 Nyeon bughan-ui daeoemuyeog donghyang [2016 Trends in North Korean Trade]," Korea Trade Investment Promotion Agency, July 27, 2017, https://news.kotra.or.kr/common/extra/kotranews/globalBbs/249/fileDownLoad/47252.do.

97. "CCDI: Liaoning vice governor under investigation," CGTN, November 23, 2017, https://news.cgtn.com/news/7a417a4e78637a6333566d54/share_p.html.

98. Li Keqiang, "Full Text: *Report on the Work of the Government (2016)*," State Council of the People's Republic of China, March 17, 2016, http://english.gov.cn/premier/news/2016/03/17/content_281475309417987.htm.

99. Adam Taylor and Min Joo Kim, "North Korean Economy Suffers Its Steepest Decline in Two Decades," *The Washington Post*, July 20, 2018, https://www.washingtonpost.com/world/north-korean-economy-suffers-steepest-decline-in-two-decades/2018/07/20/50a84dbc-8bd7-11e8-8b20-60521f27434e_story.html?utm_term=.d9cd8b2eb7fb.

100. Emily Rauhala and Damian Paletta, "China Warns It Could Fire Back with Tariffs on $60 Billion in U.S. Goods," *The Washington Post*, August 3, 2018, https://www.washingtonpost.com/world/asia_pacific/china-warns-it-could-fire-back-with-tariffs-of-60-billion-in-us-goods/2018/08/03/57ffbf56-9716-11e8-8ffb-5de6d5e49ada_story.html?utm_term=.0a69399bffe8.

101. The State Council of the People's Republic of China, "China's Arab Policy Paper," January 13, 2016, http://english.gov.cn/archive/publications/2016/01/13/content_281475271412746.htm; "Arms Control and Proliferation Profile: China," Arms Control Association, July 2017, https://www.armscontrol.org/factsheets/chinaprofile.

102. Kenley Butler, "Weapons of Mass Destruction in Asia," The Nuclear Threat Initiative, October 1, 2002, https://www.nti.org/analysis/articles/weapons-mass-destruction-central-asia/.

103. Samuel Ramani, "North Korea's Military Partners in the Horn of Africa," The Diplomat, January 6, 2018, https://thediplomat.com/2018/01/north-koreas-military-partners-in-the-horn-of-africa/.

104. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 2345 (2017)*, S/2018/171 (March 5, 2018), http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171.

105. United Nations Security Council, *Report of the Panel of Experts Established Pursuant to Resolution 2145 (2017)*, S/2017/742 (September 5, 2017), http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/131.

106. United Nations Security Council, *Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)* (February 27, 2017), http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150.

107. United Nations Security Council, *Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)* (February 23, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=S/2015/131.

108. Kevin Sieff, "North Korea's Surprising, Lucrative Relationship with Africa," *The Washington Post*, July 10, 2017, https://www.washingtonpost.com/world/africa/north-koreas-surprising-lucrative-relationship-with-africa/2017/07/10/c4e6f65d-30fe-4bd2-b178-d90daaac3007_story.html.

109. Financial Action Task Force, *Mutual Evaluation Report: Anti–Money Laundering and Combating the Financing of Terrorism: The Federal Democratic Republic of Ethiopia* (May 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/WB-ESAAMLG-Mutual-Evaluation-Report-Ethiopia-2015.pdf.

110. While exact figures vary, the U.S. State Department estimates that North Korea dedicated about 24 percent of its gross domestic product to military expenditure. U.S. Department of State, *World Military Expenditures and Arms Transfers 2017* (December 2017), https://www.state.gov/t/avc/rls/rpt/wmeat/2017/index.htm.

111. Financial Action Task Force, *Mutual Evaluation Report: Anti–Money Laundering, Ethiopia*.

112. Hamish Macdonald, "Ethiopia Working to Restrict North Korean Embassy's Bank Accounts: MFA," NKNews.org, August 3, 2017, https://www.nknews.org/2017/08/ethiopia-working-to-restrict-north-korean-embassys-bank-accounts-mfa/.

113. "Export Scheme Charges Unsealed in U.S. District Court," The U.S. Attorney's Office Middle District of Pennsylvania, press release, April 2, 2014, https://www.justice.gov/usao-mdpa/pr/export-scheme-charges-unsealed-us-district-court.

114. Brewer, "Study of Typologies of Financing of WMD Proliferation."

115. Don Oberdorfer, "Pakistan: The Quest for Atomic Bomb," *The Washington Post*, August 27, 1979, https://www.washingtonpost.com/archive/politics/1979/08/27/pakistan-the-quest-for-atomic-bomb/a0488214-1603-41f4-b168-8ba45057a10b/?noredirect=on&utm_term=.093aafdc4f73; Alex Wagner, "Bush Waives Nuclear-Related Sanctions on India, Pakistan," Arms Control Association, October 1, 2001, https://www.armscontrol.org/act/2001_10/sanctionsoct01.

116. Richard Boucher, daily press briefing, U.S. Department of State, September 24, 2001, https://2001-2009.state.gov/r/pa/prs/dpb/2001/5040.htm.

117. "Improving Global AML/CFT Compliance," Financial Action Task Force.

118. Drazen Jorgic, "China Lends $1 Billion to Pakistan to Boost Plummeting FX Reserves – Sources," Reuters, June 30, 2018. https://www.reuters.com/article/us-pakistan-china-loans/china-lends-1-billion-to-pakistan-to-boost-plummeting-fx-reserves-sources-idUSKBN1JQ0TV.

119. U.S. Department of State, *Country Reports on Terrorism 2017* (September 2018), https://www.state.gov/j/ct/rls/crt/2017/282845.htm; "FATF Unhappy with Pakistan's Efforts to Combat Terror," *Deccan Herald*, October 11, 2018. https://www.deccanherald.com/international/faft-team-not-happy-pakistans-697445.html.

120. Catherine Collins and Douglas Frantz, "The Long Shadow of A. Q. Khan," *Foreign Affairs*, January 31, 2018, https://www.foreignaffairs.com/articles/north-korea/2018-01-31/long-shadow-aq-khan; Declan Walsh, "Disgraced Atomic Scientist Disowns Confession," The Guardian, May 29, 2008, https://www.theguardian.com/world/2008/may/30/pakistan.nuclear.

121. "Arms Control and Proliferation Profile: Pakistan," fact sheet (Arms Control Association, July 2018), https://www.armscontrol.org/factsheets/pakistanprofile.

122. 1540 Committee, "Pakistan," United Nations 1540 Committee, http://www.un.org/en/sc/1540/assistance/offers-of-assistance/offers-from-member-states/pakistan.shtml.

123. U.S. House of Representatives, *Empowering Financial Institutions to Fight Human Trafficking Act of 2018*, H.R. 6729, 115th Cong., 2nd sess., https://www.congress.gov/bill/115th-congress/house-bill/6729/text?q=%7B%22search%22%3A%5B%22information+sharing%22%5D%7D&r=13.

124. Brewer, "Study of Typologies of Financing of WMD Proliferation."

125. For example, Wells Fargo's presentation at the ACAMS annual meeting in Las Vegas in September 2017, session titled: "A Clear and Present Danger: Developing Models to Combat Proliferation Financing."

126. Wenxin Fan, Tom Wright, and Alistair Gale, "Tech's New Problem: North Korea," *The Wall Street Journal*, September 14, 2018, https://www.wsj.com/articles/north-koreans-exploit-social-medias-vulnerabilities-to-dodge-sanctions-1536944018.

127. "Treasury Targets North Korea-Controlled Information Technology Companies in China and Russia," U.S. Department of the Treasury, press release, September 13, 2018, https://home.treasury.gov/news/press-releases/sm481.

128. Julia Solomon-Strauss, Edoardo Saravalle, and Claire Groden, "Uncharted Waters: A Primer on Virtual Currency Regulation around the World" (Center for a New American Security, October 2018), https://www.cnas.org/publications/reports/uncharted-waters.

129. Alan Juhn, "Hong Kong Regulator, Banks Launch Blockchain-Based Trade Finance Platform," Reuters, July 17, 2018, https://www.reuters.com/article/us-blockchain-trade/hong-kong-regulator-banks-launch-blockchain-based-trade-finance-platform-idUSKBN1K70AP.

130. Figure is based on Project Alpha Report on Typologies of Financing of Proliferation, October 2017, which is based on the 2017 Final Report of the U.N. Panel of Experts on DPRK. This figure is reprinted from Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation," (Center for a New American Security, January 2018), 9.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy.

CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

1152 15th Street, NW Suite 950 Washington, DC 20005
t. 202.457.9400 | f. 202.457.9401 | info@cnas.org | cnas.org

Bold. Innovative. Bipartisan.