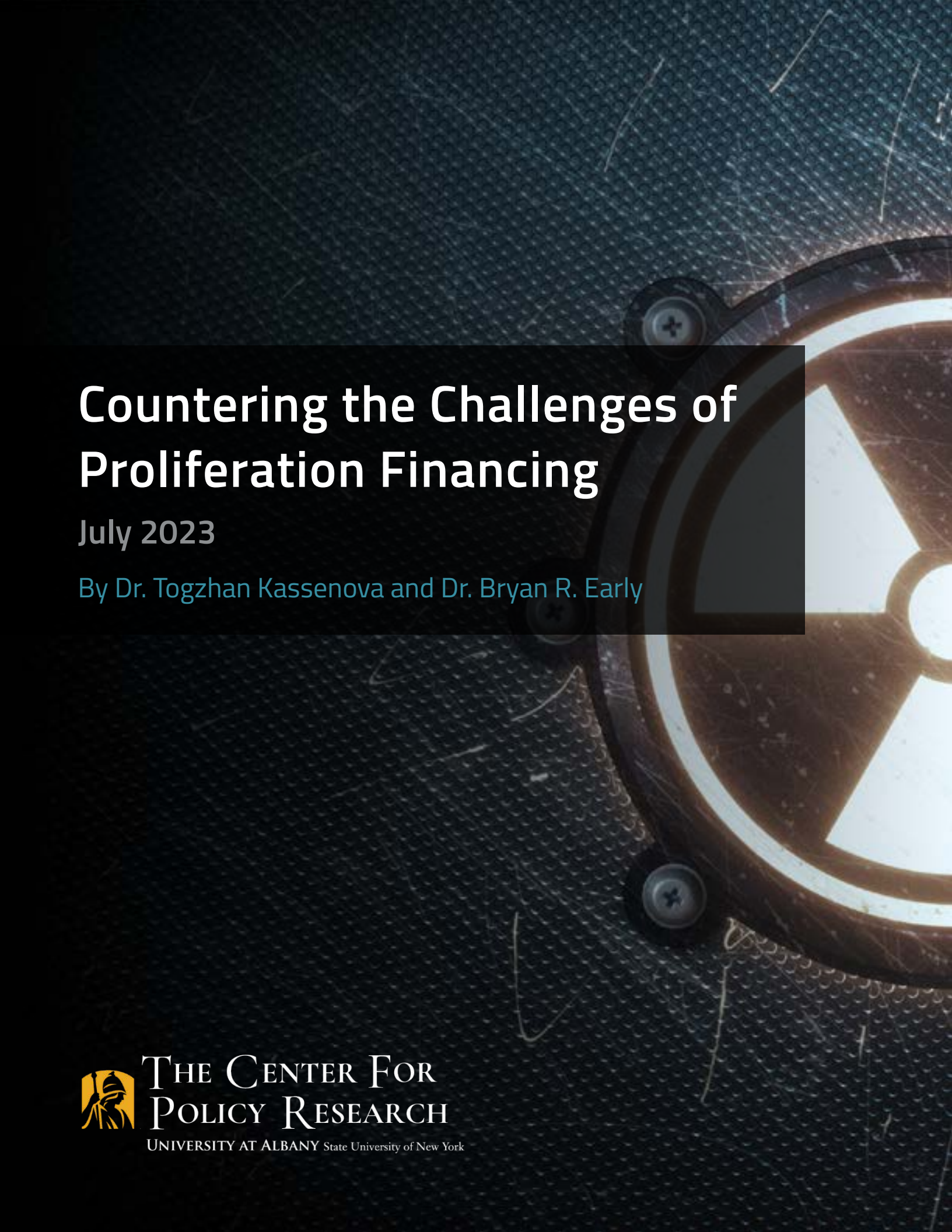

Countering the Challenges of Proliferation Financing

July 2023

By Dr. Togzhan Kassenova and Dr. Bryan R. Early

The Center For Policy Research
University at Albany State University of New York

Countering the Challenges of Proliferation Financing

July 2023

By Dr. Togzhan Kassenova & Dr. Bryan R. Early

The Center For Policy Research
University at Albany State University of New York

About the Authors

Dr. Bryan R. Early is a Professor of Political Science and Associate Dean for Research at the University at Albany, SUNY's Rockefeller College of Public Affairs Policy. Dr. Early is also the founding director of the Project on International Security, Commerce, and Economic Statecraft (PISCES). He has expertise on economic sanctions, weapons of mass destruction security issues, shadow economies, and political violence.

Dr. Togzhan Kassenova is a Washington, DC-based Senior Fellow with the Center for Policy Research (CPR) at University at Albany and a Nonresident Fellow with the Nuclear Policy program at the Carnegie Endowment for International Peace. She is an expert on nuclear politics, WMD nonproliferation, and financial crime prevention.

About the Project on International Security, Commerce, & Economic Statecraft (PISCES) at the Center for Policy Research

The PISCES Team at the Center for Policy Research possesses world-class expertise on the topics of strategic trade controls, economic sanctions, nonproliferation, and proliferation financing. Comprised of a core team of seven experts with legal, academic, and policy backgrounds, PISCES has worked with over three dozen governments around the world on nonproliferation and economic statecraft issues. The PISCES Team has helped governments with drafting strategic trade control laws, enhancing regulations, training personnel, facilitating industry outreach, and utilizing red teaming to counter-proliferation threats. PISCES team members also conduct both academic and policy research to help understand how to employ strategic trade controls, proliferation financing controls, and economic sanctions effectively.

Project on International Security, Commerce, and Economic Statecraft
Center for Policy Research
Rockefeller College of Public Affairs & Policy
University at Albany, SUNY
1400 Washington, Ave.
Albany, NY 12222

Acknowledgments and Statement of External Interests

We would like to thank the Smith Richardson Foundation for funding this research project. At the University at Albany, Dr. Keith Preble and Dr. Keon Weigold provided research assistance in support of this report. We are also grateful to the over three dozen experts that we interviewed for this report who freely shared their perspectives, knowledge, and expertise with us. We also appreciate the feedback provided by numerous experts in the field on previous drafts of this report.

Via their sponsored work at the Center for Policy Research, Dr. Bryan Early and Dr. Togzhan Kassenova have been the recipients of cooperative agreements from the U.S. State Department's Bureau of International Security and Nonproliferation to provide international training and outreach on proliferation financing risks and controls. No U.S. government funds were used to support this research. All views expressed are the authors' own.

Table of Contents

Introduction

If a 10-kiloton nuclear bomb, the same type North Korea tested in 2013, is detonated over Washington, DC, estimated fatalities will exceed 54,000 people, and injuries will exceed 86,000 people. The nuclear fireball will reach 650 feet into the sky, and anything within it will vaporize. Radiation, thermal, and light blast damage will cover miles.[1] Such a nuclear detonation in any part of the world will bring devastation of unimaginable scale.

Nuclear weapons are not the only weapons that can cause mass casualties. Biological and chemical weapons can cause mass destruction and horrific suffering. The Syrian government's use of the chemical agents sarin and chlorine against its population in 2013–14 demonstrates the mass casualty threat such weapons pose. Recent foreign assassination attempts linked to the Russian government against Sergei Skripal and Alexei Navalny both employed Novichok nerve agents, an alternative application of deadly poisons.[2]

State actors are not the only ones who can potentially use weapons of mass destruction (WMD). Nonstate actors and terrorist groups can employ mass terror. In the past, Al Qaeda and, more recently, the Islamic State professed their interest in weapons of mass destruction. The Japanese secret cult Aum Shinrikyo dispersed sarin at Tokyo underground stations, killing thirteen and injuring 5,800 people.[3] In 2001, a disgruntled American bioscientist sent anthrax letters to U.S. media figures and politicians.[4]

Neither states nor terrorist groups can procure a ready-to-use weapon of mass destruction on the international market. What proliferators can procure is technology, equipment, and material that can help them with an illicit weapons program. In most cases, the goods and technologies they buy are dual-use: useful for both legitimate commercial applications and potential military purposes. For example, an aluminum alloy of a specific grade is a valuable material for building satellites used for science. Still, it can also be used to build a missile or centrifuges for uranium enrichment.

Export controls are designed to regulate trade in sensitive goods. By requiring companies to seek permits or licenses for trade involving sensitive goods, governments minimize the risk that such goods will end up in the wrong hands or be used for illicit purposes. Export controls are essential in preventing the proliferation of weapons of mass destruction, but they are not foolproof. Proliferators have learned how to circumvent export controls and employ tricks to deceive suppliers and governments.[5]

Nonproliferation-related sanctions punish the most notorious proliferators—states (e.g., North Korea),

companies, and individuals. Nonproliferation sanctions typically include an export control component (restrictions on buying sensitive goods) and a financial component (targeted financial sanctions that impose asset freezes on designated entities and individuals as well as other financial restrictions). While the United States has more actively employed the threat and imposition of sanctions in support of its nonproliferation objectives,[6] the international use of nonproliferation sanctions has been limited to only a small number of known proliferators, such as Iran and North Korea, making this tool insufficient for addressing broader proliferation concerns.

For a long time, the focus of counterproliferation efforts remained on the procurement of goods and technology with the help of export controls but without much thought about the financial transactions that underpinned it. Over the last decade, the financial component of proliferation-related procurement came to be seen in a higher resolution. It is now recognized that cutting proliferators' access to financial services is essential in fighting proliferation.[7] Without the ability to raise and use the money to pay for illicit procurement, proliferators will face more obstacles in carrying out illicit activities. Conceptually, systems designed to cut financing for proliferation can be called *proliferation financing controls.* Developing and adopting policies that will help build and implement proliferation financing controls on the ground remains a challenge.

This report explores how the private sector, governments, and international bodies can counter illicit proliferators' exploitation of the international financial system in their efforts to acquire WMD and their means of delivery. Our report draws on the analysis of over fifty proliferation financing cases collected for this project and eight national case studies in jurisdictions with varying levels of proliferation financing controls.[8] We also interviewed over three dozen experts from governments, the private sector, and the policy community, online and in person. Beyond the United States, these included field visits to Australia, France, and the United Kingdom in 2022-2023. Through triangulating our understanding of proliferation financing threats, the perspectives of experts, and the policies of governments and international bodies to counter those threats, we seek to explain the key challenges that exist for implementing effective proliferation financing controls and offer recommendations for overcoming them.

Our report identifies several key challenges preventing the adoption of more robust proliferation financing controls. One of the most significant impediments to the implementation of more effective proliferation financing controls is the lack of consensus in defining what constitutes proliferation financing. Additionally, a narrow approach for implementing proliferation financing controls focuses primarily on UN Security Council–targeted financial sanctions against Iran and North Korea.[9] Third, we discuss how the siloing of policies and practitioner communities that address export controls and financial crimes hampers more effective imposition of proliferation financing controls. Fourth, we evaluate the practical

challenges associated with implementing proliferation financing controls on the ground that can both create resistance to their adoption and limit their impact.

We do not view the challenges associated with adopting effective proliferation financing controls in a vacuum from politics, the broader challenges facing the nonproliferation regime, and the unintended consequences of obligating the private sector to take preventative measures against financial crimes. The challenges associated with promoting more effective proliferation financing controls exist within broader debates about the stymied progress of global disarmament efforts and political conflict between great powers. Promoting the enhanced use of proliferation financing controls should also not significantly contribute to the harmful externalities of anti–money laundering, countering terrorist financing and sanctions compliance efforts like de-risking, which have isolated vulnerable populations in conflict zones and the developing world from the global economy. We think these issues are important to highlight, as they should play an essential role in determining the best strategies for improving how proliferation financing controls can be used.

In the final section of our report, we outline a series of recommendations that flow from our analysis and from interviews with experts for improving the adoption of proliferation financing controls. Some of our recommendations are easier to adopt. In contrast, our recommendation of pushing to establish a broader definition of proliferation financing nested within the soft-law obligations of the Financial Action Task Force (FATF) will take an enormous investment of time, resources, and diplomatic energy. In sum, we think that proliferation financing controls can and should be implemented more effectively to counter global risks pertaining to the proliferation of weapons of mass destruction and their means of delivery. Building an enhanced understanding of proliferation financing threats, channels for communication and cooperation between stakeholders, and more efficient approaches for the financial sector to implement proliferation financing controls are all critical to preventing proliferators' exploitation of the financial industry.

Building a System for Proliferation Financing Controls: Policy Shortcomings

Gaps in International Legal Instruments

The first conceptual problem concerns the gaps in existing international legal instruments that require countries to develop proliferation financing controls. The international obligations on proliferation financing primarily come from two sources: the UN Security Council resolutions and the Financial Action Task Force (FATF) Recommendations.

UN Security Council resolutions: Legal power but no enforcement "teeth"

Let's imagine that a national system of proliferation financing controls is a house that each country must build in accordance with international standards. The international standards for the house's foundation are broad enough and rely on the international norms against illicit WMD programs and legally binding UN Security Council resolutions.

It is a universally accepted norm that countries must not seek illicit programs of weapons of mass destruction. The Biological Weapons and Toxin Convention bans biological weapons. The Chemical Weapons Convention bans chemical weapons. The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) recognizes only five countries as nuclear-weapon states—the United States, Russia, the United Kingdom, France, and China. Most countries joined the NPT as non-nuclear-weapon states and promised not to seek nuclear weapons. These three broad regimes establish the norm against the proliferation of weapons of mass destruction.

The United Nations Security Council resolutions adopted under Chapter VII of the UN Charter are legally binding on all UN member-states. A handful relate to the nonproliferation of weapons of mass destruction: UN Security Council Resolution 1540 (2004) and its subsequent iterations, Iran-specific UN Security Council Resolution 2231 (2015), and several North Korea–specific UN Security Council resolutions adopted between 2006 and 2017.

UN Security Council Resolution 1540 (2004) requires that all UN member-states establish national measures to prevent the domestic or foreign acquisition, proliferation, and use of WMD by nonstate actors. The UN Security Council adopted the resolution in the aftermath of the 9/11 attacks, when it

became clear that nonstate actors were ready to inflict harm on a massive level, including with WMD. Al Qaeda, the terrorist group behind 9/11, had also publicly expressed an interest in procuring nuclear weapons. Other incidents mentioned above, in addition to Iraqi insurgents' bombing of chlorine gas trucks, added to the pressure to prevent nonstate actors from acquiring WMD.

UN Security Council Resolution 1540 referred to "financing" as part of proliferation controls. The follow-up resolution 2325 (2016) noted the need for more attention on proliferation finance measures. It was the first UN Security Council resolution to mention "proliferation finance" explicitly, but it did not define the term. In 2022, another follow-up, UN Security Council Resolution 2663 (2022), upheld and encouraged compliance with the proliferation financing component of the UN Security Council Resolution 1540.[10] During the comprehensive review of UN Security Council Resolution 1540 in 2022, some member-states advocated for including the definition of "proliferation financing" in the new UN Security Council Resolution 2663 (2022). The effort failed due to opposition from certain states.

North Korea and Iran are under heightened scrutiny from the international community for nonproliferation reasons. In 2003, North Korea withdrew from the NPT and announced it had a nuclear weapons program; in 2006, it tested its first nuclear weapon. In response, the United Nations Security Council imposed sanctions. Since 2006, the UN sanctions regime against North Korea, designed to prevent Pyongyang's advancement of nuclear and missile programs, has significantly expanded. North Korea–specific UN Security resolutions have created the broadest UN sanctions regime ever. In addition to targeted financial sanctions, the UN sanctions regime against North Korea includes many restrictions, including sectoral sanctions, broad financial prohibitions, and bans on the import and export of specific goods.

Unlike North Korea, Iran does not have nuclear weapons, but its nuclear program has been a source of concern for the international community. In response to Iran's violation of international nuclear safeguards—compromising the ability of the International Atomic Energy Agency (IAEA) to have confidence in the peaceful nature of Iran's nuclear program—the UN Security Council adopted several resolutions against Iran. In 2015, under the Iran Nuclear Deal, formally known as the Joint Comprehensive Plan of Action (JCPOA), Iran agreed to curtail its nuclear activities and open its program to greater scrutiny. In response, the UN lifted nuclear sanctions against Iran. Importantly, while the UN Security Council Resolution 2231 (2015) was adopted to reflect the change, it also kept in place restrictions on Iran's missile activities, established rules for the controlled supply of nuclear goods necessary for Iran's civilian nuclear program, and maintained a list of targeted financial sanctions.

Combined, the UN Security Council resolutions provide basic standards on what a house foundation should look like. Under the UN Security Council Resolution 1540, UN member-states must have

national proliferation controls (broad interpretation, not specific to any country). Under country-specific UN Security Council resolutions on Iran and North Korea, UN member-states must abide by special restrictions imposed on Iran and North Korea.

Despite the UN Security Council resolutions constituting hard international law for UN member-states, there is no mechanism to punish lack of implementation. If we use our house-building analogy, the UN Security Council resolutions provide general rules on how to build a house, but if countries add less cement, use weaker metal, or use shorter reinforced concrete structures for the foundation of their house, there is no UN mechanism to enforce the implementation of even basic standards. Persistent evasion of the UN sanctions by proliferators can be attributed to the lack of capacity and/or political will in countries worldwide. When countries do not fully implement the UN Security Council resolutions, the United Nations is limited in how it can enforce its standards.

FATF: Enforcement "teeth" but limited concept of proliferation financing

The Financial Action Task Force (FATF) is an intergovernmental organization that sets standards in the field of financial crime prevention and uses peer stakeholders to inspect compliance with its standards. Suppose we continue with our house construction metaphor. In that case, FATF acts as a cement authority and a house inspector, determining how cement must be mixed and applied and inspecting and reporting on how it is done at a specific building site. FATF adopted a list of forty Recommendations addressing various components of financial crime prevention—money laundering, terrorism financing, and proliferation financing.

Unlike the UN Security Council resolutions, FATF's Recommendations are not *hard* but *soft* law. They do not represent legally binding requirements. At the same time, unlike the United Nations, FATF and regional FATF-style organizations can visit countries and assess the quality of the house. FATF's mutual evaluation process checks how individual countries comply with FATF Recommendations, providing an effective enforcement mechanism of "naming and shaming." No country wants to find itself on FATF's "grey" or "black" lists or receive low compliance ratings from FATF.[11] As one industry expert we interviewed surmised, FATF's Recommendations "have teeth."

Implementing proliferation financing controls is among the forty broad standards that the FATF has adopted. FATF's standards on proliferation financing are limited and require less from countries than the equivalent of all relevant UN resolutions and, indeed, less than is necessary to cast a wider net against proliferators. FATF's Recommendation 7 requires countries to implement Iran- and North Korea–specific *targeted financial sanctions*. In other words, FATF adopted only one component of the relevant UN-

imposed controls. Such a narrow scoping of Recommendation 7 leaves out potential proliferators not designated by the UN Security Council and not associated with North Korea or Iran. Jurisdictions pay close attention to FATF's standards as FATF has an enforcement mechanism. The narrow scope of FATF's standards on proliferation financing is a missed opportunity to encourage countries to develop and implement broader proliferation financing controls.

In a sign of greater attention to the issue, in 2020 FATF revised two recommendations to include a proliferation financing component. Recommendation 1 was expanded to call on countries to conduct proliferation financing risk assessment (in addition to previously required assessments on money laundering and terrorism financing) and to compel their regulated institutions to do the same. The scope of the required proliferation financing risk assessment is tied to Recommendation 7 and the UN's targeted financial sanctions only. Recommendation 2 on interagency cooperation and coordination now also includes proliferation financing, in addition to money laundering and terrorism financing.

In summary, the UN provides a sufficient legal basis for countries to adopt comprehensive proliferation financing controls but has no way to enforce them. FATF has the means to enforce its Recommendations, but the Recommendations fall short of what would be necessary for comprehensive proliferation financing controls.

Lack of a Universally Accepted Definition of Proliferation Financing

The lack of a universally accepted definition of proliferation financing further complicates the mismatch between the scope of the UN Security Council resolutions, FATF Recommendations, and broader proliferation financing concerns. FATF's working definition sums up proliferation financing as follows:

> "Proliferation financing" 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.[12]

In 2021, FATF Guidance on Proliferation Financing Risk Assessment and Mitigation included the following explanation in a footnote:

> The financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).[13]

The lack of a universally accepted legal definition of proliferation financing and the limited focus of FATF Recommendation 7 on targeted financial sanctions creates a situation in which jurisdictions and financial institutions are left to decide what they understand as "proliferation financing."

The most common interpretation among relevant stakeholders in many countries is that proliferation financing controls equate to the implementation of targeted financial sanctions against Iran and North Korea. This limited understanding means that most jurisdictions are not developing and implementing policies that address broader proliferation risks, including risks from other potential proliferant states and proliferators (entities and individuals) who are not currently sanctioned. FATF's revised Recommendation 1 also limits the required national risk assessment to assessing risks connected with targeted financial sanctions against Iran and North Korea. It should be noted that many Iran- and North Korea–specific risk assessment practices could be relatively easily adapted for broader proliferation risk assessment.[14]

Both the legislation in many countries analyzed for this study and our interviews with the private sector representatives confirm this trend. Often, implementing domestic legislation focuses on the targeted financial sanctions—updating details on the establishment of domestic lists, procedures to reflect changes to the UN lists, and procedures on freezing assets of designated entities and individuals, and so on. This leaves domestic legislation unprepared to minimize risks associated with proliferators who are not designated. Many private sector representatives interviewed for this study commented that proliferation financing was "in the sanctions bucket."

Siloed Approach

Proliferation financing is directly tied to the flow of sensitive dual-use goods, and the primary objective of proliferation financing controls is to prevent financial flows that could help with illicit procurement. Export controls are designed to prevent illicit procurement. In that sense, proliferation financing controls should tie in with export controls as the two types of controls reinforce each other.

Export control actors, such as export licensing agencies, customs authorities, border control, and others, have substantially more expertise on dual-use goods than financial institutions ever will. They have data on flows of sensitive goods, companies, and individuals involved in strategic trade, including suspicious actors. This information can be extremely valuable to the financial sector as it tries to prevent proliferators from accessing the financial system. In turn, the financial sector (private and public actors) has information that export control actors cannot see. For example, financial actors can identify how a specific entity or individual is connected financially to other entities and individuals. If export control authorities and financial actors combine their efforts, they can more efficiently identify proliferation networks.

In practice, the two types of control—if they exist—are rarely tied to each other in many countries. Many jurisdictions tack on proliferation financing to anti–money laundering and counter-terrorist financing, keeping proliferation financing controls separate from export controls (if an export controls system even exists). What does this siloed approach mean in practice?

It means that the legal-regulatory basis is not calibrated to connect two mutually reinforcing forms of national controls of proliferation. In most cases, countries added the words "proliferation financing" to the existing legislation on combating money laundering and terrorism financing. In some cases, legal provisions can be found in the legislation relevant to the implementation of UN sanctions. Secondary legislation (rules and regulations) also does not connect financing controls to more goods-focused controls. As a result, at the institutional level, there are no clear ways for export control authorities and financial crime prevention authorities to act in tandem.

Problems with Implementation on the Ground

Challenges with implementing proliferation financing controls on the ground stem from two sources. First, limitations at the policy level translate into circumscribed approaches for financial institutions to prevent proliferation. Limited awareness that the UN Security Council Resolution 1540 requires proliferation financing controls, heightened focus on country-specific (Iran/North Korea) UN Security Council resolutions, and FATF's narrow focus on targeted financial sanctions against Iran and North Korea trickle down to limited understanding and weak implementation of proliferation financing controls by the financial actors.

Second, financial institutions run into capacity limitations when it comes to implementing proliferation financing controls. The capacity problem is especially acute for small- and medium-sized financial institutions that do not have strong compliance teams. Proliferators' deception techniques make it even harder for financial institutions to fulfill their obligations to implement sanctions and proliferation financing controls. The following section presents the most common practical problems with implementing proliferation financing controls and highlights lessons learned from known proliferation financing cases.

Common Problems with Implementing Proliferation Financing Controls

Reliance on list screening

Screening against lists of sanctioned entities and individuals (UN, EU, or unilateral sanctions) remains the main tool used by financial institutions to weed out proliferators. While necessary to perform, list screening has its limitations and cannot be considered an effective tool for implementing sound proliferation financing controls if employed on its own.

List scanning by financial institutions generates a high number of false positives. Common names and similar-sounding names clog up the system. Clearing flagged names and transactions takes time away from conducting other risk management measures, and financial institutions can do little to minimize the problem. An even more serious problem is that once designated, entities and individuals begin hiding behind associates' names and front or shell companies. List-scanning software cannot detect that form of deceit.

Limited information on transactions and goods, and deception

Financial institutions have limited information on the goods behind transactions. They cannot know with certainty what is being sold and usually cannot identify if dual-use goods are involved. For example, a wire transfer for dual-use equipment can say "spare parts" or "laboratory equipment." Even if some information about the goods is available, financial institutions cannot distinguish legitimate trade in dual-use goods from proliferation activity.

The fact that proliferators engage in deception makes the task even harder. Proliferators and agents working on their behalf lie about end-use, end-users, and final destinations. What looks like a piece of equipment going to a research institution to promote science can turn out to be a case of illicit procurement for the benefit of an illicit weapons program.

Some financial institutions in jurisdictions with advanced financial sectors, such as the United States, are trying to bring on board specialists who can identify risky transactions. They recognize that it is hard to detect proliferation-relevant transactions by relying solely on the documentation taken at face value. This is especially true if proliferators operate through a well-established network and intend to trans-board the cargo.[15]

Customer due diligence and transaction monitoring do not account for proliferation financing

In most cases, standard customer due diligence and transaction monitoring procedures do not incorporate a proliferation financing component except for sanctions-related list screening. The analysis of secondary legislation (rules and regulations), government guidance for the private sector in case-study countries, and interviews with private sector actors about their practices conducted for this study confirm the trend. So far, actionable compliance and risk management measures are more suitable for preventing money laundering, terrorism financing, and the implementation of targeted financial sanctions. Financial institutions also struggle to identify front and shell companies used by proliferators, making it possible for a designated entity or individual to continue using financial services despite being sanctioned.

The analysis of known proliferation financing cases in the subsequent section demonstrates that, in some cases, more careful customer due diligence measures could have ensured the timely discovery of proliferation networks. For example, companies operating from the premises of a North Korean embassy or trade representative office could have been flagged as potential procurement and financial agents working on behalf of North Korea if their addresses had been checked more closely.

Difficulties with automating

Representatives of financial institutions interviewed for this study emphasized the need for automation and the operationalization of proliferation financing typologies. Automating alerts for proliferation financing is considerably more challenging than for money laundering and terrorism financing. Amounts involved in proliferation financing are usually modest (unlike large amounts in money laundering), and trade transactions look like legitimate commercial activity. Unless the entities or individuals are sanctioned, it is hard to detect proliferation-relevant activity.

If we look at proliferation financing as consisting of both procurement and fundraising, we should acknowledge that spotting and automating alerts for fundraising for WMD programs is even more challenging than spotting and automating alerts for procurement. Identifying a link between fundraising and proliferation activity is next to impossible.

Unintended Consequences

Proliferators and the individuals, entities, and illicit networks working on their behalf often manage to escape being caught. Meanwhile, those with nothing to do with proliferation find themselves denied services due to de-risking. De-risking is directly tied to the private sector's challenges with implementing proliferation financing controls and economic sanctions. When an institution is not confident about its risk assessment and risk mitigation measures, it tends to de-risk (to avoid anything that can potentially be associated with prohibited activities or entities).

The negative impact of extreme de-risking is twofold: it imposes hardships on nontarget groups and negates the policy effectiveness of sanctions. The example of two proliferation-related sanctions regimes (Iran and North Korea) illustrates the point.

Even after the adoption of the Joint Comprehensive Plan of Action (JCPOA), some private sector actors worldwide continued to de-risk Iran-related activities. The withdrawal of the United States from JCPOA under President Trump and the reintroduction of U.S. unilateral nuclear sanctions against Iran, including secondary sanctions on non-U.S. entities, further deterred international banks and companies from engaging with Iran. De-risking, in this case, has an adverse impact on the population in terms of growing poverty rates, restricted access to medications, and environmental consequences. The negative policy impact is significant. Hardliners within Iran promote the idea that JCPOA did not bring Iran economic

benefits and push Iran to relinquish its commitments under the JCPOA. At the time of writing, the situation surrounding Iran's nuclear activities and JCPOA's future remains fluid. In response to the US withdrawal from JCPOA, Iran stopped implementing several of its JCPOA commitments, thus increasing nuclear risks for the international community.[16]

Broad UN and unilateral sanctions against North Korea result in a significant adverse impact on the North Korean population. Negative consequences include fuel shortages, lack of electricity, and hardships for civil transport and agriculture. The UN Panel of Experts on North Korea documented a loss of 200,000 jobs due to sectoral sanctions.[17] While actors engaged in illicit activities on behalf of North Korea manage access to global financial systems thanks to deceit, humanitarian organizations find it more and more difficult to provide humanitarian assistance to North Korea as financial institutions refuse to offer their services despite an exemption for humanitarian assistance under the UN sanctions regime. The net effect of overcompliance and de-risking is devastating for the vulnerable parts of the North Korean population.

Adopting a more nuanced approach, one that differentiates between prohibited activities and permitted transactions for humanitarian or other activities, will positively affect the well-being of vulnerable groups and the policy impact of sanctions regimes.

Another reason for de-risking is fear of sanctions enforcement actions by the U.S. government. The United States maintains the world's broadest sanctions regime, which goes beyond UN sanctions. Concerns over losing access to the U.S. financial system push private financial institutions in third countries to disengage fully from any Iran- or North Korea–related transactions.

Uncomfortable Questions

What appears to be a technocratic question of proliferation financing controls does not exist in a vacuum. Rather it is part of a complicated global context: the tension between nuclear disarmament and nonproliferation; lack of political will among some key players to promote proliferation financing controls; and a question mark over whether other states, beyond North Korea and Iran, must be seen as proliferators.

Global Nuclear Order: Tensions between Disarmament and Nonproliferation

Today, there are roughly 13,000 nuclear weapons in the world, 90 percent of which are in the hands of the United States and Russia. Three additional states—China, France, and the United Kingdom—collectively hold almost 900 nuclear weapons. These five countries are recognized as nuclear states under the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). Four additional countries—Israel,[18] Pakistan, India, and North Korea—possess nuclear weapons while remaining outside of the NPT. North Korea abandoned the NPT in 2003 and developed advanced nuclear and missile programs. Israel, Pakistan, and India never joined the NPT to begin with. Iran has an advanced nuclear program and, at least in the past, engaged in military research in the nuclear field.

The NPT "bargain" centers on the promise that, in return for access to peaceful nuclear technology, non-nuclear-weapon states will never seek nuclear weapons, and that nuclear-weapon states will move toward disarmament. As of 2023, the global nuclear order is under strain. States without nuclear weapons are disillusioned with the lack of progress of the five nuclear-weapon states (United States, Russia, the UK, France, and China) toward disarmament; likewise, they see no indication that the other four countries (Israel, Pakistan, India, and North Korea) plan to give up their nuclear programs. The Treaty on the Prohibition of Nuclear Weapons (TPNW), adopted by the UN in 2017 and in force since 2021, has been ratified by sixty-eight countries.[19] The treaty indicates global dissatisfaction with the progress of nuclear disarmament efforts.

The tension between most non-nuclear-weapon states and the nine states with nuclear weapons has direct implications for promoting nonproliferation objectives. Many developing non-nuclear-weapon states ask, "Why do we have to invest our limited resources in strengthening nonproliferation controls when a few countries keep their nuclear weapons and do not plan to disarm?" The perceived unfairness of the global

nuclear order has a detrimental effect on the buy-in and sustainability of nonproliferation goals and objectives. It also leads parties to deflect responsibility for preventing additional proliferation, viewing it as the responsibility of those states that do possess weapons of mass destruction.

Elephants in the Room

The implementation of the UN Security Council nonproliferation sanctions and the strengthening of proliferation financing controls depend on the political will and consensus within the UN Security Council. The uncomfortable truth is that not all members of the Security Council are on the same page regarding the implementation of nonproliferation sanctions. Question marks persist on whether China is doing enough to prevent North Korean sanctions evasion originating within China. Similarly, experts point out Russia's leniency when it comes to North Korea and its open cooperation with Iran in contravention of UN Security Council Resolution 2231.[20]

Another uncomfortable question is: Who counts as a proliferant state? North Korea and Iran are the focus of proliferation financing controls for a reason. Should they be the only ones? Should the discourse on proliferation financing confront questions about other actors? For example, should the Syrian government, which procured chemical agents on the international market and used chemical weapons against its own people, be discussed more often in the context of proliferation financing concerns? What about countries with nuclear weapons but outside the NPT, such as India, Pakistan, and Israel? While those countries never agreed to be bound by the NPT, their decisions to acquire nuclear weapons still create significant security and proliferation challenges.

Russia's Use of Chemical Agents, Inhumane Munitions, and the War against Ukraine

Russia's annexation of Crimea in 2014 and its full-scale invasion of Ukraine in 2022 led to a wide range of international sanctions on Russia. In 2014, major economies, including the United States, the United Kingdom, and the European Union, restricted, among other things, Russia's ability to import dual-use goods. In 2021, in response to the use of chemical weapons against its citizens (most recently, the use of a Novichok agent against opposition leader Alexei Navalny), the U.S. government imposed additional sanctions on Russia that cut access to controlled goods and technology, arms financing, and assistance.[21]

After the 2022 invasion of Ukraine, the United States, the United Kingdom, the European Union, and several other countries imposed further restrictions on the export of dual-use goods to Russia.

In addition to coordinated efforts across more than three dozen countries, the United States imposed export controls on items that could be useful for Russia's chemical and biological weapons production capability. Increasingly, Russia is moving into a category of states whose procurement of dual-use goods and technology is restricted, which raises questions about controls over financing in support of such procurement. Since 2022, some financial institutions have begun stopping commercial outgoing and incoming wires involving Russia and the parts of Ukraine occupied by Russia—that is, putting a temporary hold on such transactions in order to request invoices.

Russia has also employed weapons of war, ballistic missiles, cruise missiles, and unmanned aerial vehicles (UAVs) in attacks targeting civilians and civilian infrastructure in Ukraine. Ukraine has claimed, and evidence supports, that Russia has employed indiscriminate white thermite munitions against Ukrainian civilian populations.[22] These weapons, which inflict severe burns, are considered inhumane, and targeting civilians with them should be considered a war crime. Russia has also employed advanced delivery systems with both conventional and potentially WMD applications to target Ukrainian cities and Ukraine's energy infrastructure. Russia is forthright in admitting that its missile and UAV strikes have sought to cut off Ukrainians from heat and electricity during the winter months.[23] Should any financial transactions involving aerospace or semiconductors that enable Russia to buy or build missiles and UAVs also be considered subject to proliferation financing restrictions? Should applying proliferation controls against proliferation fundraising efforts apply to Russian oil sales that fund its military? The international community's ambiguous definition of proliferation financing and inconsistent implementation of proliferation financing controls mean that no clear prerogatives exist to do so.

Proliferation Financing Cases: Trends and Tactics

Known cases of proliferation financing can provide valuable data on the tactics and methods used by proliferators. It is important to remember that what comes to light does not represent the full picture. Discovered and disrupted cases may yield insights into some tactics used by proliferators, but the newest and most effective tactics may be associated with undetected transactions—and, as such, unknown.

North Korea

North Korea is a convenient case to analyze tactics for financing illicit WMD programs. As discussed earlier, there is no universally agreed definition of proliferation financing. It remains an open question of what kind of transactions can be strictly defined as proliferation financing. Broadly defined, proliferation financing can include two components—fundraising and procurement. Fundraising is harder to identify. Does it have to be proven that part of the funds raised went toward a weapons program? Or is the fact that funds benefit the proliferant state enough to assume that part of these funds goes to the weapons program?

In North Korea's case, this dilemma is minimized. A comprehensive UN sanctions regime provides a legal foundation for implementing controls on North Korea's fundraising in addition to North Korea's procurement of sensitive items. Over the years, the scope of UN sanctions on North Korea has expanded from controls directly tied to its WMD program—restrictions on importing sensitive goods that could help with its nuclear and missile programs—to controls over the generation of funds for the North Korean regime. North Korea is banned from selling commodities ranging from seafood to statues. Pyongyang is banned from sending workers overseas to earn income. More importantly, the UN Security Council imposed broad restrictions on North Korea's access to global financial services. In North Korea's case, UN sanctions align with the broad definition of proliferation financing and even go beyond it.

Another reason North Korea serves as a good case study is the data availability. Thanks to the UN Panel of Experts, media reporting, and open-source information, it is possible to collate enough cases to identify trends and common methods of evasion. To understand North Korea's tactics and methods, we analyzed known cases of North Korea's illicit procurement and fundraising in violation of UN sanctions. In almost every case, North Korean agents used multiple evasion tactics. Below we highlight the most common tactics used in illicit procurement and fundraising.

Illicit procurement

Use of front companies, accounts under false names, falsified documentation

In most cases analyzed for this study, North Korea's agents relied on front companies. The case of Mun Chol Myong—the first North Korean citizen to be extradited to the United States—provides a good example.[24] Mun Chol Myong engaged in money laundering on behalf of North Korean entities, including the sanctioned ones. He also supplied and sourced materials for Glocom, a Malaysia-based company controlled and operated by North Korea's Reconnaissance General Bureau (North Korea's intelligence arm). Mun Chol Myong and his conspirators relied on a network of Singapore-based front companies and bank accounts registered under false names. They removed references to North Korea from wire transfers and transaction documents. Such deceitful techniques helped Mun and his associates deceive U.S. correspondent banks.[25]

In another case of note, Taiwanese agents supplied sensitive WMD-related goods to North Korea. One of the involved individuals, Alex H. T. Tsai, a citizen of Taiwan, forged shipping invoices to facilitate the illegal transfer of sensitive goods procured in the United States via Taiwan to North Korea. Payments came from Taiwan to U.S. financial institutions. After the U.S. government designated Tsai and the companies he controlled, he and his associates continued to conduct business under new company names.[26]

The case of the Foreign Trade Bank (FTB), a North Korean bank designated by the United Nations, United States, United Kingdom, and European Union for its role in advancing North Korea's nuclear and missile program, shows the scale of the deception. FTB used more than 250 front companies to evade sanctions. FTB's agents maintained multiple accounts under false names. As a result, China's Bank of Dandong processed more than $2.5 billion in U.S. dollar transactions between 2012 and 2015 through U.S. correspondent accounts.[27]

Use of foreign companies as procurement and payment agents

North Korea uses legitimate foreign companies to facilitate procurement and payment on its behalf. The example of Singapore's Chinpo Shipping Company is a good example. Chinpo, established in 1970, for years facilitated the activities of North Korea's Ocean Maritime Management (OMM) after the United States sanctioned OMM. Chinpo carried out financial transactions on behalf of OMM through a Singapore branch of the Bank of China. Chinpo's head, Tan Cheng Hoe, also helped North Koreans find employment in Singapore and helped resolve disputes between North Korean and Singaporean businesses. Chinpo

also offered office space to the North Korean embassy.[28] Chinpo's activities came to light when Panama's authorities seized the vessel *Chong Chon Gang*, which was carrying conventional weapons to North Korea; Chinpo had paid for the vessel to transit via the Panama Canal. In this case, those who were helping North Korea relied extensively on the tactics of false documentation and fraud. The transaction involved an invalid bill of lading, OMM's role in sourcing the funds sent to Chinpo was obscured, and, to avoid the Bank of China's scrutiny, the name of the shipping vessel was not included in the wire transfers associated with the payments. This case illustrates the sophisticated schemes that proliferators engage in to hide the illicit nature of their transactions from financial institutions.

Use of diplomatic personnel and individuals with diplomatic passports

Using diplomatic cover for illicit procurement is a signature tactic of the North Korean regime.[29] North Korean diplomats and individuals with North Korean diplomatic passports engage in the illicit procurement of sensitive goods and use their bank accounts to carry out payments for procurement and to transfer funds on behalf of the North Korean regime.

The Munitions Industry Department (MID), sanctioned by the UN since 2016 for its role in nuclear and missile programs, has been involved in various sanctions evasion schemes, from illicit procurement to sending IT workers overseas. MID used procurement agents masked as diplomatic officers in the North Korean missions and trade offices, in addition to third-country nationals and foreign companies.[30]

In a 2018 case, German media—NDR TV—ran an investigative report suggesting North Korean diplomats in Berlin used the embassy to procure technology for North Korea's nuclear and missile programs.[31] Earlier, in 2016–17, another German media outlet—public broadcaster ARD—reported that German intelligence observed efforts by North Korean officials to procure technology and equipment. The head of German intelligence, Hans-Georg Maasen, confirmed that "procurement activities have been carried out" in support of nuclear and missile programs.[32]

Fundraising

North Korea relies on selling goods and services overseas to raise funds for the regime. Part of the raised funds goes to North Korea's nuclear and missile programs. Sources of funds include income from the sale of conventional weapons, drugs, and other commodities, overseas labor, cybercrime, the hospitality business, and use of diplomatic premises, to name a few.

Sale of art, conventional weapons, drugs, and other commodities

North Korea generates funds overseas from selling art, conventional weapons, drugs, and other commodities. The sale of North Korean art generates millions in revenue. For example, in 2016 alone, North Korea's Mansudae company and its affiliated galleries generated $260 million.[33] In 2019, South Korean authorities seized Mansudae art at Incheon airport.[34] North Korean art can be found in galleries and showrooms across the world.[35] The sale of military equipment is another lucrative business for North Korea. North Korea does not discriminate and sells conventional weapons to state and nonstate actors across the world, from Eritrea to Russia. For example, in 2017, the UN Panel of Experts reported on a 2016 interdiction of North Korean military equipment bound for Eritrea via China.[36] In 2022, North Korea was accused of selling arms to a Russian mercenary group fighting in Ukraine.[37] Illicit drug sales bring substantial funds to the North Korean regime as well. The extent of North Korea's drug operations was demonstrated in the 2003 case of the freighter *Pong Su* that attempted to bring nearly $100 million in heroin into Australia.[38]

Overseas labor: Infrastructure projects

Revenue from overseas labor serves as a significant revenue stream. It helps prop up Kim Jon Un's regime and contributes funds to nuclear and missile programs. Despite the UN ban on North Korea's overseas labor, Pyongyang continues to insert its citizens into various revenue-generating projects. Historically, popular sectors for North Korea's overseas labor included IT, hospitality (e.g., hostels, restaurants), construction, and medical fields.

A common method for North Korea to supply labor is via establishing joint ventures in third countries, often with the help of front companies. This happens even though the UN sanctions regime prohibits joint ventures with North Korea's participation. One of the real-life examples involves the North Korean art-focused enterprise described above, known under the names of Mansudae Overseas Project/Mansudae Art Gallery/Mansudae Art Studio. In addition to producing and selling art, Mansudae often serves as a front company for North Korea's joint ventures in other countries. It exports labor, with the company's presence documented across many African countries (Botswana, the Democratic Republic of Congo, Equatorial Guinea, Ethiopia, Mali, Mozambique, Namibia, Senegal, Zimbabwe).[39]

In Namibia alone, North Korea allegedly earned $66.3 million for the construction of the presidential palace, a cemetery for national heroes, and the Independence Hall.[40] Cash earned by Mansudae's overseas operations was deposited in local banks, then withdrawn, divided into smaller amounts, and carried back to North Korea.[41] In Senegal, entities linked to Mansudae via a front company called Corman

Construction earned income for North Korea by managing construction projects. Despite Senegal refusing visas to its employees, Mansudae's people continued to operate and maintain bank accounts in Senegal.[42] In the Democratic Republic of Congo, two North Korean nationals registered a company called Congo Aconde SARL to facilitate construction projects. Their methods of storing and moving the money involved opening accounts in U.S. dollars in a Lubumbashi branch of a bank headquartered in Cameroon. Three additional individuals also opened similar accounts. The turnover of their transactions reached $400,000.[43]

Another case provides additional clues into the methods of earning, moving, and handling cash from overseas labor. Korean Rungrado General Trading Company sent construction workers to countries across the world, including China, Qatar, the United Arab Emirates (UAE), Mongolia, the Czech Republic, Poland, Bulgaria, Saudi Arabia, Cambodia, Namibia, and other countries in Africa. Earned cash was initially deposited in local banks before being withdrawn and carried to North Korea in suitcases.[44]

Overseas labor: IT workers

Income from North Korean IT workers operating overseas provides a steady flow of income for the North Korean regime. While not their main activity, IT workers also facilitate cyberattacks conducted by North Korean actors. North Korean workers register on freelance platforms under false identities. They perform various IT-related tasks, such as the development of websites and applications. Part of their income covers their presence overseas, and the rest is channeled back to North Korea. The Korea Computer Center (KCC) case provides an example of how North Korea raises funds via overseas IT labor and cyberattacks. KCC is a state-run R&D center that develops software and programming, such as the "Red Star" operating system and software for controlling man-made and armament systems.[45] KCC has been outsourcing IT labor to third countries like Russia and China. In 2017, the U.S. Office on Foreign Assets Control (OFAC) sanctioned KCC.

Cybercrime and the crypto domain

Cyberattacks generate substantial revenue for Pyongyang's nuclear and missile programs. The most common tactics North Korean actors use include cyber-enabled financial theft and money laundering, extortion with ransom demands, and cryptojacking (stealing cryptocurrency from other users and cryptocurrency exchanges). North Korean hackers are extremely entrepreneurial in conducting cybercrime heists, which can include sophisticated social engineering techniques.

North Korea is responsible for some of the world's most notorious cybercrime cases. In 2014, North Korean

cyber agents attacked SONY Pictures, stole confidential data, and damaged thousands of computers. In 2016, North Korean actors stole $81 million from the Bangladesh Bank. Since 2016, North Korean actors have organized fraudulent ATM cash withdrawals around the world.[46]

North Korea increasingly relies on the crypto domain. It uses cyberattacks to steal, launder, and move virtual assets to fund its illicit activities, including to support its nuclear and missile programs. Known cases of North Korea's cyber-enabled cryptocrime speak volumes about the scale of the problem. In 2022 alone, North Korea was confirmed to have stolen cryptocurrency worth millions of U.S. dollars. In March of that year, the North Korean-affiliated Lazarus Group was responsible for stealing $100 million in cryptocurrency from an online video game network. In June 2022, the Lazarus Group and its agents stole $100 million in cryptocurrency assets from Harmony Horizon Bridge.[47] In December 2022, South Korean intelligence reported that since 2017, North Korea had stolen cryptocurrency assets worth $1.2 billion globally.[48]

The hospitality business and the use of embassy properties

Until the German authorities shut it down in 2020, the City Hostel Berlin (CHB) earned the North Korean government 40,000 euros a month (500,000 euros per year in rental income alone from an on-site conference center). The North Korean government received the building as a gift from the former East German Communist government during the Cold War.

The Berlin city government first tried to shut down the hostel in 2017. The German federal government attempted to close it in 2018 as it drew a link between the income generated by the hostel and the funding of North Korea's nuclear program. The hostel operators argued that they stopped making payments to the North Korean regime in 2017, a claim that the German court doubted to be true.[49] The hostel operators, who routinely invoked the property's diplomatic status to placate local police, later lost their appeal against the hostel's closure.[50] In 2020, the hostel was finally shut.[51]

Iran

As of 2023, Iran is the only country, other than North Korea, to find itself under country-specific proliferation-relevant UN Security Council resolutions. Iran's case has differences and similarities with North Korea's case. The restrictions on Iran under the UN umbrella are not as broad as on North Korea. Iran is much better integrated into a world community, including in the economic sphere. Unlike North

Korea, Iran does not possess a nuclear weapon but has an advanced nuclear program that does provide latent nuclear capability. Like North Korea, Iran and agents acting on its behalf procure sensitive goods and technology on the international market and use the global financial system to make payments.

After the adoption of the JCPOA, the UN Security Council passed Resolution 2231 (2015), which terminated all previous UN Security Council resolutions targeting Iran's nuclear program. Under the new Resolution 2231, the UN Security Council requested that states use an official procurement channel application process to regulate Iran's imports of goods, technology, and materials for Iran's nuclear activities under the JCPOA. A special JCPOA Joint Commission reviews supply proposals and makes recommendations to the UN Security Council. The UN Security Council makes decisions. Some nuclear-related activities do not require approval by the Security Council, for example, when goods and technology are exclusively for use in light-water reactors.

The UN Security Council retained the arms embargo on Iran for five years after implementation (until 2020 or until the IAEA submitted a report confirming the Broader Conclusion that all nuclear material remained in peaceful activities) and sanctions on Iran's ballistic missile program for eight years (until 2023 or until the IAEA submits a report confirming the Broader Conclusion). The UN-mandated arms embargo on Iran was lifted in 2020 in accordance with the resolution's five-year provision, but the missile restrictions remain in place at the time of writing.

The UN Security Council Resolution 2231 prohibits making assets or financial services available or conducting financial transactions related to certain nuclear-related items, ballistic-missile-related items, and arms and other materiel without Security Council approval. The UN Security Council maintains a consolidated list of Iranian individuals and firms subject to sanctions for violating missile restrictions. As of 2023, the list included sixty-one sanctioned entities and twenty-three sanctioned individuals.[52]

In Iran's case, the legal foundation for clamping down on the fundraising component of proliferation financing is less straightforward. Unlike in the North Korean case, the UN Security Council does not impose broad restrictions on Iran's economic activity. With that in mind, our analysis focused on the patterns in illicit procurement and payment methods.

Several patterns are associated with Iran's illicit procurement and payment mechanisms in support of sensitive procurement. On the procurement side, individuals and entities often rely on domestic orders that do not require an export license for further reshipment to Iran, ordering of items that fall under the controlled threshold but can still be useful in a weapons program, use of false end-user information, use of front companies, and use of same individuals acting as owners of several companies located in different

countries (for example, the same person owns both the company in the United States that puts in an order for a sensitive item and the company in a third country that is used as an intermediary receiver of the item). Once items are procured, they are often shipped via third countries, mislabeled, or mixed in with noncontrolled items.

On the payment side, Iranian agents employ the following methods: use of payment intermediaries, payments under $10,000 to avoid scrutiny, use of money exchanges, attempts to switch wires for noncontrolled items to pay for controlled items, use of third countries for payment transfers, use of code words in payment instructions to avoid scrutiny, use of correspondent accounts, and other methods. We chose three case studies below to showcase the above methods.

The case of Shahab Ghasri: Swedish valves destined for Iran

Shahab Ghasri, based in Sweden, used his company Petroinstrument HB to procure sensitive goods from European suppliers for the benefit of Iran. Ghasri received payments from Iran via a money exchange company in Sweden and a wire transfer to a Swedish bank. Swedish authorities initially noticed Petroinstrument HB as a result of the suspicious activity reports filed by banks in late 2010 and early 2011. In 2011, Ghasri arranged to ship corrosion-resistant valves to a customer in Iran. Ghasri indicated Sharjah, UAE, as the end-use destination for the valves, only to change the air waybill to Iran at the last minute. Swedish authorities intercepted the shipment and searched his home and office where they found documents related to previous transactions. In 2013, a Swedish court found Ghasri guilty and gave him a three-month suspended jail sentence.[53]

U.S. aluminum tubes for Iran via Belgium and Malaysia

In 2007, an Iranian individual, owner of Super Alloys LLC in the UAE and NBH Industries in Malaysia, sought to procure aluminum tubing from the United States for the benefit of Iran. The plan was to order cylinders on behalf of Super Alloys LLC in UAE and then reexport them to Iran. Aluminum cylinders can be used in the production of uranium enrichment centrifuges. Super Alloys LLC also attempted to procure various noncontrolled metals and sent a $30,000 wire to pay for them. Once the supplier received the wire, Super Alloys LLC tried to use some of the transferred money to pay for controlled aluminum tubes instead. The Iranian individual claimed that the aluminum end-users would be oil companies located in the UAE.

The United States denied the U.S. supplier a license for the export of cylinders from the United States

to the UAE. In response, the individual devised a scheme to route the items via Europe and Malaysia and onward to Iran. In 2009, he recruited Nicholas Kaiga, a European businessman, to assist. Kaiga was the managing director of Industrial Metals & Commodities. His company address was a residential neighborhood, suggesting it was likely a front company. Kaiga ordered cylinders while providing false end-user information that named a Belgian company, Aerospace Industrial Metals & Commodities (registered at the same residential address as Industrial Metals & Commodities), as a receiver. The Iranian individual and Kaiga did not realize that the U.S. government monitored their communication. Kaiga received the goods in Belgium and reshipped them to NBH Industries in Malaysia. It then turned out that NBH Industries existed in a virtual office. On request from the U.S. government, the U.S. supplier provided goods of lower technical specification, not suitable for centrifuges. Kaiga was arrested in the United States in 2013 and sentenced to twenty-seven months in prison and two years of supervised release after deportation.[54]

Karl Lee: A Chinese national supplying Iran with sensitive goods [55]

One of the most notorious and long-term cases of Iran-related proliferation financing involves a Chinese national known as Karl Lee. Lee operated and likely continues to operate in Dalian, China, despite having been sanctioned internationally. Lee began supplying Iran with sensitive goods in defiance of UN sanctions beginning at least in 2004 with the help of shell and front companies. Lee both procured goods from different manufacturers on behalf of Iran and sold goods manufactured at the facilities he was associated with.

The main company initially associated with Lee was LIMMT Economic and Trade, established in 1998. In 2006, the U.S. government added LIMMT to its Specially Designated Nationals List (SDN) list; in 2009, it added Karl Lee himself. Since LIMMT was sanctioned, no U.S. financial institution was allowed to provide financial services to the company. But since most of its financial transactions clear in U.S. dollars and touch the U.S. financial system, Lee had to devise ways to deceive the system.

Lee directly instructed his customers to use alias names and new account numbers for LIMMT to avoid having transactions blocked. Unsuspecting non-Iranian importers of Lee's products also received similar instructions to use various alias names instead of LIMMT and ever-changing account numbers. In 2008, the U.S. government indicted LIMMT on 118 counts, including for supplying false business information to financial institutions.

Lee established a new set of front companies in response to U.S. sanctions and the Chinese government's clampdown on setting up companies in his own name. He then used the names of his family members

and close associates to open multiple accounts to transfer funds. He even used the name of his late mother. Many of these companies used LIMMT's address or a close variant. According to available data, between 2006 and 2014, Karl Lee carried out more than 165 separate USD transactions worth $8.5 million in violation of U.S. sanctions. It is worth remembering that proliferation-related transactions often involve modest amounts and might not trigger the attention of financial institutions, but over time they can add up to substantial amounts that benefit proliferation. According to press reports, between 2009 and 2013, Lee earned $10 million. Undeterred, Lee continued setting up new companies that he used for his illicit activities. As with the previous networks Lee set up to evade sanctions, the companies' names, owners' names, and addresses are often the same.

Comparing the Two Proliferation Financing Cases

North Korea and Iran constitute the two cases in which a strong legal obligation exists to impose restrictions on financial transactions that could contribute to nuclear and missile proliferation. Deception is a key tactic employed in proliferation financing in both cases. The more comprehensive nature of the sanctions programs against North Korea made a broader set of transactions potentially subject to proliferation financing controls under the auspices of UN Security Council sanctions. Additionally, those policies drove a larger share of North Korea's fundraising activities into more illicit criminal activities. In North Korean case, crimes pay for proliferation. Iran's proliferation activities are able to interface more easily with legitimate commercial partners (though still relying on deception) because its economy is not as isolated, especially after the JCPOA. When fundraising activities fall under the aegis of proliferation financing controls, a significantly broader range of behaviors constitute violations and may be subject to disruption. North Korea's reliance on criminal behavior also provides justification for seeking to disrupt and punish its fundraising activities beyond the proliferation financing angle. When the strategy for imposing proliferation financing controls focuses more narrowly only on proliferant transactions, the detection of cases becomes much harder.

Given the unlikeliness of achieving another comprehensive international sanctions regime as stringent as the one against North Korea in the foreseeable future, Iran is likely to be the more generalizable case. Governments and financial institutions face the challenge of identifying when Iranian agents are seeking to circumvent nonproliferation sanctions and strategic trade controls rather than simply trying to deny Iranians access to any financial transaction. Preventing this type of proliferation financing requires governments and financial institutions to have access to more significant amounts of information about transactions as well as the analytical abilities to determine which ones are legitimate.

Policy Recommendations

Over the last decade and a half, the international community has started paying more attention to proliferation financing controls. The UN Security Council Resolution 1540 (2004) included a reference to proliferation financing, and subsequent resolutions have reiterated the call to UN member-states to implement proliferation financing controls. The UN Security Council resolutions on Iran and North Korea have provisions directly relevant to proliferation financing controls. The introduction of FATF Recommendation 7 in 2012 and the inclusion of the proliferation financing component in FATF's work made a noticeable difference. In 2020, FATF further strengthened the proliferation financing component by revising Recommendations 1 and 2 and requiring proliferation financing national risk assessments and national interagency coordination and cooperation in implementing proliferation financing controls. The progress on the international front must be lauded. At the same time, the shortcomings identified in this study, including the lack of a universal definition of proliferation financing and opposition to the expansion of FATF's Recommendations and stronger language on proliferation financing within the UN Security Council Resolution 1540 context, point to a challenging international policy environment.

Based on the analysis of proliferation financing cases and the challenges with implementing proliferation financing controls, we propose the following recommendations for consideration by relevant stakeholders.

Develop primary and secondary legislation

Many jurisdictions lack legal provisions for the comprehensive implementation of proliferation financing controls. Before developing new or revising existing legislation, national governments should consider the following questions:

- What will be the scope of proliferation financing controls? Targeted financial sanctions or broader proliferation financing controls? What will be the definition and interpretation of *proliferation financing* in domestic legislation?
- Will proliferation financing controls be integrated with the prevention of financial crime (anti–money laundering and counterterrorism financing), prevention of terrorism, export controls, and implementation of UN Security Council resolutions (e.g., UN Law)?

In an ideal scenario, as a minimum, countries must ensure that domestic legislation fully reflects the UN Security Council resolutions and is not limited to implementing the targeted financial sanctions. Without

domestic legal provisions, the full implementation of the UN Security Council resolutions is impossible.

Provisions on how UN designations of entities and individuals are translated into domestic implementation should be specific, especially on timing. For example, provisions such as "implementation 'without delay'" or "'regularly' updating domestic lists based on new UN designations" should be time specific.

If a country adopts a broad definition of proliferation financing, the legislation should include provisions that accommodate it. For example, legal provisions should allow for risk management, detection, disruption, investigation, and prosecution of proliferation financing cases involving state and nonstate actors other than Iran and North Korea. All standard components of legislation—key implementing agencies, authorities, and obligations, sanctions for violation, provisions for interagency cooperation and coordination, and information-sharing—must be clearly defined.

Conduct national proliferation financing risk assessment

FATF revised Recommendation 1 calls on countries to conduct proliferation risk assessments tied to the implementation of targeted financial sanctions (in line with FATF Recommendation 7). *FATF Guidance on Proliferation Financing Risk Assessment and Mitigation* (2021) provides a good starting point for a risk assessment.[56] Depending on the national approach to proliferation financing controls, a country might conduct a broader risk assessment not limited to targeted financial sanctions.[57] Academic institutions[58] and technical assistance donors can help countries with more comprehensive proliferation risk assessment.

Governments should conduct national risk assessments as soon as feasible because national risk assessments can provide a foundation for financial institutions to carry out institution-specific risk assessments. Governments should conduct private sector outreach specific to risk assessment, especially targeting smaller or medium-sized institutions with limited internal expertise and compliance resources.

Develop guidance and offer training for the private sector on how to conduct proliferation financing risk assessment and on how to include proliferation financing component in Know-Your-Customer (KYC) procedures and transaction monitoring

It would be helpful if governments developed guidance and offered training for the private sector on how to conduct proliferation financing risk assessment and how to include proliferation financing component in KYC and transaction monitoring. Small- and medium-sized institutions do not have the capacity to self-generate relevant risk assessments and risk management systems without some guidance. Even larger financial institutions that have the capacity to spend substantial resources on compliance can benefit from

some government input on these issues. So far, in most cases where governments offer guidance to the private sector, it is limited to implementing targeted financial sanctions.

As the first step, and in light of FATF's new requirement on proliferation financing risk assessment, governments should engage in industry outreach on conducting institution-specific risk assessments. The risk management system will depend on the individual institution's risk exposure and risk appetite. Quantitative and qualitative factors will feed into risk assessment to determine if there is a concentration of risk and its volume. A financial institution processing a high volume of transactions involving proliferation risk and specializing or concentrating in products, services, transactions, customers, or geographic locations at a high level of inherent risk for proliferation must invest in the technology and compliance capacity.

Understanding inherent proliferation financing risk will dictate the types of controls needed. Each financial institution needs commensurate controls to arrive at an acceptable level of residual risk. It bears remembering that the size of a financial institution does not directly correlate to the level of risk, as proliferators are keen to exploit not only major banks but small- and medium-sized banks as well. In other words, a small- or medium-sized bank with a high inherent risk must ensure sufficient controls.

There are practical steps that financial institutions can take that would help with minimizing proliferation financing risks. Such measures include but are not limited to the following:

- More detailed information on the customer's line of business at onboarding and request for additional information as part of service suitability for higher-risk services and products. For example, the United States, Canada, and Mexico use the North American Industry Classification System (NAICS) to classify business establishments. Questions that can guide the development of better-tailored customer profiles include the following: What industries can be considered sensitive (e.g., specific metals, advanced electronics, etc.)? What kind of business establishments (corporations, private companies, government-owned entities) are at higher risk? What other customer metrics (e.g., parties, counterparties, intermediaries, government-owned, etc.) are important? Financial institutions might consider including export control-related questions as part of the onboarding process. For example, financial institutions can consider asking prospective customers to self-identify: Does your business fall under export control regulations? If applicable, does your company have an internal compliance program to mitigate risks of orders for illicit procurement?
- During onboarding, it would be prudent to identify the type of accounts that should receive extra scrutiny as part of transaction monitoring (e.g., businesses trading in sensitive goods, North

Korean diplomats, individuals, and entities that can be associated with sanctioned activities, sectors vulnerable to proliferation financing and sanctions evasion such as shipping companies, trading houses, exchange houses, cryptocurrency exchanges). More broadly, financial institutions can consider the following question when developing KYC and transaction monitoring systems: What other customer metrics are important to counter proliferation? Parties, counterparties, intermediaries, government-owned, etc.?

- Financial institutions should create a risk matrix for products and services, understanding which of them are most commonly used by proliferators (wires, trade finance, correspondent banking).
- Use of additional lists during customer onboarding and transaction monitoring in addition to those legally required (e.g., lists provided by other countries, lists of suspicious entities and individuals).
- Scrutiny of additional identifying information such as physical addresses, IP addresses, and phone numbers at onboarding and as part of transaction monitoring. As discussed earlier, front companies acting on behalf of proliferators change names but often keep the same addresses, phone numbers, or managers.
- Special procedures are applicable to North Korean citizens, especially diplomats. These procedures can include confirming the period of diplomatic accreditation and tying the life period of an account to the period of accreditation, making sure no multiple accounts are opened by the same individual.
- Strengthening trade finance procedures to incorporate a proliferation financing component. This can include, for example, a more comprehensive check of all parties to the transaction, including brokers and shippers. Distributed ledger or blockchain can be useful as it provides information on all parties and is hard to falsify. For example, it is impossible to fake a stamp if only the customs agency can put this information into the blockchain.
- Harvesting and using unstructured data to uncover proliferation-relevant transactions. Scanning unstructured data, such as wire data, invoices, shipping documents, bills of lading, insurance documentation, customs stamps, suspicious activity reports (SARs), negative news, law enforcement requests, and so on, can provide valuable unstructured data. The data can be reorganized into a readable format and fed into a transaction monitoring system for keyword search. Obtaining such capacity, including scanners and technology, will be harder for small- and medium-sized banks.

In addition to promoting more robust KYC procedures and transaction monitoring in relation to proliferation financing controls, governments should consider emphasizing the value of uncovering out-of-pattern transactions to the private sector. As described above, the financial institutions' capacity to

detect proliferation financing will always be constrained. It is unrealistic to expect financial institutions to confidently identify proliferation-relevant transactions based on the presence of dual-use goods, as they do not have enough expertise or information. A more effective approach is to focus on out-of-pattern transactions.

A private sector representative interviewed for this study suggested a hypothetical out-of-pattern scenario. A small transistor company in the United States that sells to commercial companies starts receiving wires from intermediary countries, facilitating technology transfer to China. The pattern had been orders worth $80,000 per year; now it jumps to $80,000 per order. This can generate two types of alerts: out-of-pattern and wires from a high-risk jurisdiction. Enhanced due diligence can then turn up important additional information: "You check the website for the product price and discover that these electronics can be used in missile guidance."[59] As pointed out by the interviewee, it is not the equipment that stops a transaction but an aspect of the transaction that is out of pattern.

Minimizing silo approach: An interagency approach to proliferation financing controls

Our interviews with the government representatives in various jurisdictions revealed that there is little day-to-day coordination or information-sharing between the counterproliferation community (e.g., those dealing with export controls) and the financial crime prevention community. It appears that even in countries with more advanced systems, such coordination only happens when there is a need to respond to intelligence. For example, the government obtains intelligence on a suspicious actor and collects information across different jurisdictions.

We believe creating a system for more regular preventive risk management might be useful. In practical terms, it might include the development of standard operating procedures for sharing information on importers and exporters of sensitive goods and lists of suspicious entities. It will also help if financial institutions can request assistance from export control authorities on the technical specifications of certain goods. For example, suppose a financial institution sees that a particular type of equipment is involved in a trade finance transaction and has doubts about the transaction. In that case, it has a channel to contact the export control authorities for technical advice.

Promote exchanges and joint trainings between financial crime prevention and export control professionals

Developing mutual understanding and enhanced communication between the financial crime prevention and export control communities will not occur organically and needs to be deliberately fostered. Providing

training to export control experts on how the international financial system works, the role of the FATF, and the existing framework for preventing financial crimes will help them better understand how proliferation financing controls can contribute to implementing export controls. By the same token, financial crimes experts may have little training as to what dual-use goods are, how they contribute to proliferation, and the interagency processes for implementing and enforcing export controls. We have found that bringing members from these communities together for joint trainings to be a powerful tool for gaining buy-in and enhancing community members' expertise in implementing proliferation financing controls—at both the industry and government levels. We recommend that industry outreach efforts by governments and training programs by professional organizations and international bodies do more to promote crossover training that brings together financial crimes and export control experts.

Additionally, an important set of actors includes firms and experts who handle sanctions law cases and financial crime compliance advisory work. They could play an important role in advising and educating their clients on proliferation financing risks. As such, it would be beneficial to create opportunities for them to interact with export control, trade finance, and other relevant professionals for better awareness of proliferation risks.

We believe governments have a primary role in driving the private sector outreach and creating opportunities for the private sector to interact with relevant government actors, but it is not feasible to rely on governments alone for training opportunities. Some training should be government-led, but in some cases, governments can act as encouragers/motivators while major banks and companies can proactively create opportunities and be in charge.

Inclusion of a proliferation financing component in supervision and clear requirements for reporting entities

Governments should include a proliferation financing component in supervisory procedures. Interviews with the private sector representatives indicate that without formal supervision requirements specific to proliferation financing, financial institutions will not be motivated to strengthen proliferation financing controls. Based on our interviews with compliance professionals from the private sector, the inclusion of proliferation financing as a compliance priority seemed to be related to individual managers' familiarity with the topic and whether institutions had previously been punished for sanctions violations. In the absence of an explicit, well-defined requirement, effective corporate implementation of proliferation financing controls will be idiosyncratic and unlikely to ever go beyond FATF Recommendations.

Awareness raising, training, and incentives for prosecutors

Except in the United States, prosecutors are reluctant to take up proliferation financing and sanctions evasion cases in most jurisdictions. Lack of awareness and experience with prosecuting WMD-related cases poses a severe obstacle. Relevant government agencies should consider providing specialized training on proliferation financing for prosecutors. Experience sharing by third countries with more advanced systems that have experience in prosecuting proliferation financing–related cases can significantly help. In the United States, the ability of enforcement and prosecuting bodies to take a share of financial penalties has incentivized taking enforcement actions against sanctions and export control violators.

Establishment of public-private partnerships

Effective implementation of proliferation financing controls can benefit immensely from public-private partnerships. Proliferators rely on the private sector—the financial institutions—to finance illicit procurement. Financial institutions can access data not visible to government agencies and identify networks based on financial relationships. Government agencies have data on suspect entities and individuals and see trends in illicit activity. Public-private partnerships are cooperative forums created to facilitate information-sharing between intelligence agencies, law enforcement, and a subset of the leading firms within an industry sector. Approximately fifteen public-private partnerships exist in various countries' financial sectors, such as JMLIT in the United Kingdom, FinCen Exchange in the United States, and the Fintel Alliance in Australia. Interactions in such partnerships can help firms overcome their reluctance to share information with each other and adopt a more cooperative approach to preventing proliferation financing. As one of our interviewees surmised, "companies should not compete with each other on compliance." The forums created by public-private partnerships also provide ways for governments to share more sensitive information with industry actors about specific proliferation risks and known tactics.

Adopt an enhanced soft-law definition of proliferation financing

The lack of a consensus definition of proliferation represents one of the biggest challenges to applying more effective proliferation financing controls. In our discussions with dozens of policy experts, government officials, and compliance experts from the private sector, we asked our interviewees to define proliferation financing. We heard back almost as many different answers as the people we asked. While efforts have been made to craft an internationally accepted definition at the UN Security Council, those efforts have been stymied by parties that want to prevent the emergence of more effective proliferation financing controls.

Our recommendation is that the FATF should be the body that promotes a more comprehensive definition of proliferation financing, one that goes beyond just focusing on the targets of financial sanctions for nonproliferation purposes. We think that a definition of proliferation financing in line with the explanation provided by FATF's 2021 *Guidance on Proliferation Financing Risk Assessment and Mitigation* would be a vast improvement. The challenge for the FATF would be in translating that conceptual definition of proliferation financing into pragmatic expectations of what states and financial service providers must do to prevent it. While employing a soft-law approach for defining proliferation financing has disadvantages, it may be better for overcoming financial sector resistance to enhanced compliance responsibilities by giving more room for trial-and-error and experimentation in learning how to improve the implementation of proliferation financing controls. As FATF has already demonstrated, effective implementation of soft-law requirements is far better than unenforced and generally ignored hard-law obligations when it comes to preventing proliferation financing.

Conclusion

The continued risks posed by WMD to global security warrant the use of a wide range of policy tools to address them. Financial institutions can play a larger, important role in preventing the proliferation of WMD. Proliferators and regulators are engaged in a perpetual cat-and-mouse game in which proliferators use innovative forms of deception to circumvent sanctions and export controls. Adopting robust proliferation financing controls provides an additional layer of scrutiny and challenges that proliferators must overcome in their illicit acquisition efforts.

Existing approaches for defining proliferation financing have led to a narrow strategy of implementing proliferation financing controls against only Iran and North Korea and have emphasized the overlapping obligation of implementing United Nations Security Council targeted financial sanctions. Preventing the proliferation of WMD, especially if political gridlock prevents the use of nonproliferation sanctions in the UN Security Council in the future, requires the adoption of a broader approach to defining and implementing proliferation financing controls. It also requires financial institutions to invest in utilizing a broader set of risk-based criteria, screening procedures, and information sources in evaluating whether their transactions may contribute to proliferation. Adopting improved proliferation financing controls will require international regulators, national governments, and the private sector to coordinate more effectively with one another in addressing this challenge. Adopting a soft-law approach that obligates financial institutions to find innovative, pragmatic solutions for improving the implementation of proliferation financing controls across a wider spectrum of actors engaged in proliferation could work better than the status quo.

Explaining the importance of implementing proliferation financing controls to financial institutions and gaining their buy-in for enhanced implementation will be essential to enhancing their use. Valuable approaches for realizing those goals are the use of public-private partnerships and building bridges between the financial crime prevention and export control communities. Identifying and promoting efficient ways for financial institutions to adopt proliferation financing controls, such as through improved information-sharing and risk assessment, is one of the best options for achieving effective implementation. Financial institutions can and should play a leading role in making the world not only a more prosperous place but also a more secure one.

Endnotes

1 Alex Wellerst Alex Wellerstein, "NukeMap Simulation," 2023, https://nuclearsecrecy.com/nukemap/?&kt=10&lat=38.8946925&lng=-77.0218993&airburst=0&hob_ft=0&casualties=1&fallout=1&psi=20,5,1&zm=14.

2 Mark Krutov, "'Weapon Of Terror': A Novichok Creator Tells How Navalny Case Differs From The Skripal Attack," Radio Free Europe/Radio Liberty, September 4, 2020, https://www.rferl.org/a/russia-navalny-novichok-inventor-mirzayanov-interview/30821316.html.

3 "Aum Shinrikyo: The Japanese Cult behind the Tokyo Sarin Attack," BBC, July 6, 2018, https://www.bbc.com/news/world-asia-35975069.

4 "Amerithrax or Anthrax Investigation," FBI, 2022, https://www.fbi.gov/history/famous-cases/amerithrax-or-anthrax-investigation.

5 Glenn Anderson, "Points of Deception: Explaining How Proliferators Evade Controls to Obtain Dual-Use Goods," Strategic Trade Review 2, no. 2 (2016): 4–24. Lisa Langdon Koch, "Frustration and Delay: The Secondary Effects of Supply-Side Proliferation Controls," Security Studies 28, no. 4 (2019): 773–806.

6 Nicholas Miller, "The Secret Success of Nonproliferation Sanctions," International Security 68, no. 4 (2014): 913–44.

7 Jonathan Brewer, "Studying Typologies of Proliferation Finance," King's College London Project Alpha, 2017, https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf; David Albright, Sarah Burkhard, Spencer Faragasso, Linda Keenan, and Andrea Stricker, "Connecting the Dots Characterizing and Drawing Lessons from Tactics and Methods of Illicit Procurement to Improve Counterproliferation: Volume 1." Institute for Science and International Security, February, 2020, https://isis-online.org/uploads/isis-reports/documents/Illicit_Trade_Networks_Vol1_Connecting_the_Dots_February_2020_FINAL.pdf.

8 National case studies included one jurisdiction each in North America, Central America, the Asia-Pacific, the Caribbean, East Asia, South East Asia, and the Middle East, with two jurisdictions in Europe.

9 Also, see Aaron Arnold, "Facing the myths surrounding proliferation financing," Bulletin of the Atomic Scientists, April 11, 2018, https://thebulletin.org/2018/04/facing-the-myths-surrounding-proliferation-financing/; and Ian Stewart, Andrea Viski, and Jonathan Brewer, "Combating the Financing of Proliferation: Challenges and New Tools," Journal of Financial Crime 27, no. 4 (2020): 1107–21.

10 For example, Operative Paragraph 12 calls for more attention to numerous issues, including proliferation financing.

11 See, e.g., Louis de Koker, John Howell, and Nicholas Morris, "Economic Consequences of Greylisting by the Financial Action Task Force," Risks 11, no. 5 (2023): 81, https://doi.org/10.3390/risks11050081.

12 Combatting Proliferation Financing: A Status Report on Policy Development and Consultation, FATF, 2010, 5.

13 FATF Guidance on Proliferation Financing Risk Assessment and Mitigation, FATF, 2021, https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html, 8.

14 It is helpful that FATF Guidance on Proliferation Financing Risk Assessment and Mitigation makes this point.

15 Informed by a conversation with a representative of a major U.S. bank, June 2023.

16 In March 2023, Iran and the IAEA agreed on renewed cooperation, creating a new opening for greater transparency of Iran's nuclear activities. Source: Joint Statement by the Atomic Energy Organization of Iran (AEOI) and the International Atomic Energy Agency (IAEA), March 4, 2023, IAEA, https://www.iaea.org/newscenter/pressreleases/joint-statement-by-the-atomic-energy-organization-of-iran-aeoi-and-the-international-atomic-energy-agency-iaea.

17 UN Security Council 1718 Committee Panel of Experts, Final Report of the Panel of Experts Submitted Pursuant to Resolution 2515, S/2021/211, 2021, 59.

18 Israel maintains a policy of neither confirming nor denying the presence of nuclear weapons.

19 Treaty on the Prohibition of Nuclear Weapons, UN Office for Disarmament Affairs, https://treaties.unoda.org/t/tpnw.

20 Samuel Ramani, "Why Russia Is Openly Violating Sanctions against North Korea," Monkey Cage blog, Washington Post, April 23, 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/20/why-is-russia-openly-flouting-international-sanctions-against-north-korea/.

21 "U.S. Sanctions and Other Measures Imposed on Russia in Response to Russia's Use of Chemical Weapons," U.S. State Department, March 2, 2021, https://www.state.gov/u-s-sanctions-and-other-measures-imposed-on-russia-in-response-to-russias-use-of-chemical-weapons/.

22 Chris Jewers, "The Deadly Thermite Bombs Putin Is Using to Bring Hell to Ukraine." Daily Mail, March 13, 2023, https://www.dailymail.co.uk/news/article-11853173/The-deadly-thermite-bombs-Putin-using-bring-Hell-Ukraine.html; Matt Murphy, "Ukraine war: Russia accused of using phosphorus bombs in Bakhmut," BBC, May 6, 2023, https://www.bbc.com/news/world-europe-65506993.

23 Joshua Yaffa, "The Impact of Russian Missile Strikes on Ukraine's Power Grid," The New Yorker, February 20, 2023, https://www.newyorker.com/culture/photo-booth/the-impact-of-russian-missile-strikes-on-ukraines-power-grid.

24 In March 2023, Mun Chol Myong was deported to China. "Exclusive: US Deports North Korean Sentenced for Money Laundering to China," Voice of America, March 29, 2023, https://www.voanews.com/a/exclusive-us-deports-north-korean-sentenced-for-money-laundering-to-china/7028262.html.

25 "First North Korean National Brought to the United States to Stand Trial for Money Laundering Offenses," U.S. Department of Justice, Press Release, March 22, 2021, https://www.justice.gov/opa/pr/first-north-korean-national-brought-united-states-stand-trial-money-laundering-offenses; Indictment against Mun Chon Myong, Case 1:19-cr-00147-RC, filed on March 22, 2021, U.S. Department of Justice, https://www.justice.gov/opa/press-release/file/1379211/download.

26 "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, March 16, 2015, https://www.justice.gov/opa/pr/taiwan-businessman-sentenced-24-months-conspiring-violate-us-laws-preventing-proliferation.

27 Spencer S. Hsu and Ellen Nakashima, "U.S. Brings Massive N. Korean Sanctions Case, Targeting State-Owned Bank and Former Government Officials," Washington Post, May 28, 2020, https://www.washingtonpost.com/local/legal-issues/us-brings-largest-ever-n-korean-sanctions-case-targeting-state-owned-bank-and-senior-government-officials/2020/05/28/3b23f616-a02b-11ea-b5c9-570a91917d8d_story.html; "U.S. Indicts North Koreans, Accuses State-Owned Bank of Evading Sanctions," Reuters, May 28, 2020, https://www.reuters.com/article/us-usa-northkorea-sanctions/u-s-indicts-north-koreans-accuses-state-owned-bank-of-evading-sanctions-idUSKBN23437R; Indictment against Jo Chol Man et al., United States District Court for the District of Columbia, May 3, 2018, Case 1:20-cr-00032-RC, Document 1.

28 Eda Erol and Leonard S. Spektor, "Chinpo Shipping: A Singaporean Financial Agent of North Korea," James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey, CNS Occasional Paper no. 35, 43–45.

29 Daniel Salisbury, "Spies, Diplomats and Deceit: Exploring the Persistent Role of Diplomatic Missions in North Korea's WMD Proliferation and Arms Trafficking Networks," Asian Security 17, no. 3 (2021): 313–30.

30 "North Korea Ballistic Missile Procurement Advisory," U.S. Department of Treasury, http://home.treasury.gov/system/files/126/20200901_nk_ballistic_missile_advisory.pdf.

31 "Report: Berlin a Gateway for North Korea Nukes," DW, June 2, 2018, https://www.bbc.com/news/world-europe-42935761; https://www.dw.com/en/report-north-korea-got-nuclear-knowhow-via-berlin-embassy/a-42444825.

32 "German Spy Chief Alleges North Korea Uses Berlin Embassy for Procurement," Reuters, February 3, 2015, https://www.reuters.com/article/us-germany-northkorea/german-spy-chief-alleges-north-korea-uses-berlin-embassy-for-procurement-idUSKBN1FN0J2.

33 "North Korea and the Art of Surviving Sanctions," CBS News, November 16, 2018, https://www.cbsnews.com/news/north-korea-the-art-of-surviving-sanctions-cbsn-originals/.

34 UN Security Council 1718 Committee Panel of Experts, Mid-term Report of the Panel of Experts Submitted Pursuant to Resolution 2464, S/2019/691, 2019, 22.

35 "North Korea and the Art of Surviving Sanctions," CBS News, November 16, 2018, https://www.cbsnews.com/news/north-korea-the-art-of-surviving-sanctions-cbsn-originals/.
36 UN Security Council 1718 Committee Panel of Experts, Final Report of the Panel of Experts Submitted Pursuant to Resolution 2276, S/2017/150, 2017, 32-37.
37 "Russian Mercenary Group Bought Arms from North Korea, Says White House," PBS News Hour, December 22, 2022, https://www.pbs.org/newshour/world/russian-mercenary-group-bought-arms-from-north-korea-says-white-house.
38 Doug Struck, "Heroin Trail Leads to North Korea," Washington Post, May 12, 2003, https://www.washingtonpost.com/archive/politics/2003/05/12/heroin-trail-leads-to-north-korea/017fa657-ce96-4eae-b44e-16f9376816ff/.
39 UN Security Council 1718 Committee Panel of Experts, Final Report Submitted Pursuant Resolution 2276, S/2017/150, 2017, 44.
40 Kim Yong Hun, "Foreign Currency Earning Constructions in Africa," Daily NK, May 21, 2010, https://www.dailynk.com/english/foreign-currency-earning-construct/.
41 UN Security Council 1718 Committee Panel of Experts, Final Report Submitted Pursuant Resolution 2276, S/2017/150, 2017, 44.
42 "Despite UN Sanctions, North Koreans at Work in Senegal," Voice of America, September 24, 2019, https://www.voanews.com/a/africa_despite-un-sanctions-north-koreans-work-senegal/6176412.html.
43 "Treasury Targets DPRK Actors Illicitly Generating Revenue Abroad," U.S. Department of Treasury, Press Release, March 1, 2023, https://home.treasury.gov/news/press-releases/jy1313.
44 "Treasury Sanctions Entities Involved in Exporting Workers from North Korea," U.S. Department of Treasury, Press Release, November 19, 2020, https://home.treasury.gov/news/press-releases/sm1189.
45 Choi Sung, "North Korea Needs to Set Up Practical IT Training and Certification Systems," Korea IT Times, April 2, 2010, http://www.koreaittimes.com/news/articleView.html?idxno=8242.
46 Christopher Bring, "North Korean Hackers Ramp Up Bank Heists: U.S. Government Cyber Alert," Reuters, August 26, 2020, https://www.reuters.com/article/us-cyber-usa-north-korea/north-korean-hackers-ramp-up-bank-heists-u-s-government-cyber-alert-idUSKBN25M2FU.
47 "FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft," FBI, January 23, 2023, https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft.
48 Hyung-Jin Kim, "Seoul: North Korean Hackers Stole $1.2 B in Virtual Assets," AP, December 22, 2022, https://apnews.com/article/technology-crime-business-hacking-south-korea-967763dc88e422232da54115bb13f4dc.
49 Max Jürgens, "When Your Landlord Is North Korea," Voelkerrechtsblog, March 3 2020, http://voelkerrechtsblog.org/de/when-your-landlord-is-north-korea/.
50 Jens Kastner, "Hospitality, North Korean Style, Highlights German Dilemma," Nikkei Asia, April 8, 2020, https://asia.nikkei.com/Editor-s-Picks/Tea-Leaves/Hospitality-North-Korean-style-highlights-German-dilemma.
51 "North Korean Embassy Hostel in Berlin Shuts," DW, May 29, 2020, http://www.dw.com/en/north-korean-embassy-hostel-in-berlin-locks-its-doors/a-53622706.
52 United Nations Security Council Resolution 2231 List, United Nations, https://www.un.org/securitycouncil/content/2231/list.
53 UN Security Council 1718 Committee Panel of Experts, Final report submitted pursuant to Resolution 2049, S/2013/331, 2013, 11-12; "Swedish Man Found Guilty of Violating Iran Sanctions," Iran Watch, Wisconsin Project, August 8, 2013, https://www.iranwatch.org/our-publications/international-enforcement-actions/swed-ish-man-found-guilty-violating-iran-sanctions; "Man on Trial in Sweden for Breaking Iran Sanctions," AFP, January 16, 2013, https://www.emirates247.com/news/region/man-on-trial-in-sweden-for-breaking-iran-sanctions-2013-01-16-1.491418.
54 "Belgian Man Charged with Attempting to Illegally Export Aluminum Tubes to Malaysian Front for Individual in Iran," Press Release, United States Attorney's Office No rthern District of Illinois. Oc tober 30, 2013, https://www.justice.gov/usao-ndil/pr/belgian-man-charged-attempting-illegally-export-aluminum-tubes-malay-sian-front.
55 Daniel Liu, "Karl Lee, Where Is He Now?" October 28, 2018, Project Alpha, King's College London, https://www.kcl.ac.uk/alpha/assets/report-karl-lee-where-is-he-now-final.pdf; Grand Jury Indictment, "State of New York vs. Li Fang Wei," Supreme Court of the State of New York; "'Karl Lee' Charged in Manhattan Federal Court with Using a Web of Front Companies to Evade U.S. Sanctions," FBI, April 29, 2014, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/karl-lee-charged-in-manhattan-federal-court-with-using-a-web-of-front-companies-to-evade-u.s.-sanctions; Ian J. Stewart and Daniel B. Salisbury, "Wanted: Karl Lee," The Diplo-mat, May 22, 2014; Indictment against Karl Lee "Li Fangwei in Rem Complaint," June 2014, Southern District of New York court.
56 FA TF Guidance on Proliferation Financing Risk Assessment and Mitigation, FATF, 2021, https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html.
57 For an example of a recent broad National Risk Assessment, see Proliferation Financing in Australia: National Risk Assessment, AUSTRAC, December 2022, https://www.austrac.gov.au/sites/default/files/2022-12/AUSTRAC_Proliferation_Financing_in_Australia-National_Risk_%20Assessment_Web.pdf.
58 See, e.g., Proliferation Financing Risk Assessment resources produced by RUSI, https://rusi.org/explore-our-research/projects/proliferation-financing-risk-as-sessment.
59 Interview with a representative of a U.S. financial institution, 2022.