JANUARY 2018

THE FINANCING OF NUCLEAR AND OTHER WEAPONS OF MASS DESTRUCTION PROLIFERATION

Dr. Jonathan Brewer

Center for a New American Security

About the Author

DR. JONATHAN BREWER is an Adjunct Senior Fellow at the Center for a New American Security. He is a Visiting Professor at King's College, London, carrying out research with the Alpha Project on questions of proliferation and its financing. Between 2010 and 2015 he was the financial expert on the U.N. Panel on Iran created pursuant to Resolution 1929 (2010). Dr. Brewer was a member of the U.K. Diplomatic Service between 1983 and 2010. Duties included substantive postings overseas to Luanda (1986–88), Mexico City (1991–95), and Moscow (1998–2001) and a secondment to the Joint Intelligence Committee, Cabinet Office, London (2003–04). He was Head of Counter-Proliferation 2005–2010.

Acknowledgements

The author would like to thank Loren DeJonge Schulman, Zachary Goldman, and Elizabeth Rosenberg for their review of this report. The author would also like to thank Neil Bhatiya, Edoardo Saravalle, and Kaleigh Thomas for their assistance. Finally, the author would like to acknowledge Melody Cook and Maura McCarthy for their assistance with the production of this report.

Cover Photo
Getty and AP; modified by CNAS

THE FINANCING OF NUCLEAR AND OTHER WEAPONS OF MASS DESTRUCTION PROLIFERATION

Executive Summary

The financiers of proliferation of nuclear and other weapons of mass destruction (WMD) traditionally have been states seeking to expand their military capabilities, often in defiance of international controls or treaties such as the Nuclear Nonproliferation Treaty. The threats to international peace and stability represented by the Democratic People's Republic of Korea's (DPRK) nuclear program, and even by the relatively mature programs of India and Pakistan, are testament to the success of their financiers. Nevertheless, although experts in the international community understand how financing of WMD proliferation takes place, the international framework to counter it, based on sanctions and export control laws, is relatively weak.

Countering the financing of proliferation (FoP) should be an important foundation of U.S. counter-proliferation efforts. The United States is uniquely placed to make this a global priority. First, thanks to the global dominance of the U.S. dollar as a reserve currency and as a tool of international trade, U.S. regulators are the preeminent global financial rule-makers. Second, U.S. intelligence and financial investigation abilities are among the best in the world. Third, the United States already plays a key role in global counter-proliferation efforts. It is leading the response to the most pressing proliferation crisis today by coordinating international efforts, at the United Nations (U.N.) Security Council as well as bilaterally, to counter North Korea's WMD program. It is also trying to build a stricter sanctions regime to prevent Iran from obtaining a nuclear weapon.

The financial elements of a WMD program can be divided into three stages. During the first (program fund-raising), the proliferating state raises funds for the program through its domestic budget, perhaps supplemented with funds raised by networks overseas or by criminal activity (conducted by or on behalf of state actors). During the second stage (disguising the funds), the proliferating state transfers these funds into the international financial system. If the state is not sanctioned, this is straightforward. For states subject to comprehensive sanctions like North Korea and Iran (prior to implementation of the Joint Comprehensive Plan of Action, or JCPOA), it is a major challenge. During the third stage (procurement of materials and technology), the proliferating state uses these funds in the international financial system to pay for goods, materials, technology, and logistics needed for its WMD program. Throughout this third stage, international financial institutions (FIs) will be involved in processing the related transactions.

It is often difficult for government authorities or FIs to identify FoP. The networks of procurement agents involved may be complex and may involve front companies operating in a number of different jurisdictions. The goods and materials involved are, for the most part, standard industrial or occasionally dual-use items. The latter, although subject to controls, still may be hard to identify. For due diligence, most FIs rely on screening transactions and customers against lists of sanctioned individuals or entities. Governments and regulators generally require nothing more of FIs.

U.N. and independent experts recently have published several reports on financing of proliferation typologies, intended to assist government authorities and financial institutions to control the threat. One such report, by Project Alpha at King's College London, is a comprehensive collection of case studies for different typologies.[1] These case studies involve classic and established financial mechanisms – wire transfers, trade finance products, cash, checks, and, in a few cases, credit cards. Notably, there are no examples of virtual currencies or other new payment methods. Presumably, the proliferation networks were able to conduct their procurement and financial transfer activities by traditional means and did not need more sophisticated and anonymous financial value and storage mechanisms. It is likely that the financial signatures of any program over the next five to ten years would follow these classic patterns.

Although experts in the international community understand how financing of WMD proliferation takes place, the international framework to counter it is relatively weak.

This paper examines the international framework of controls on proliferation financing. It also identifies areas that require further work to fill current gaps in the framework and to safeguard the international community against future WMD proliferation threats. The global players involved in this response will include the U.N. Security Council, the Financial Action Task Force (FATF), the Egmont Group (an informal network of Financial Intelligence Units [FIUs]), multilateral export control regimes, and national authorities.

Background

As with every area of economic activity, illicit WMD proliferation programs require financing. This requirement creates an opportunity. The financial signature or trail of a proliferation program may be a way for government investigators, banks, or trade professionals to recognize a proliferator and act to halt or disrupt its activities. "Following the money" is a proven method to track down financial criminals. To date, "following the money" has found infrequent use in a counter-proliferation context, yet it potentially could serve as a key strategy.

Very few states follow this approach, primarily because of an underdeveloped international legal framework. The U.N. resolution underpinning the international system of controls on WMD proliferation, U.N. Security Council Resolution 1540 (2004), makes only two references to financial controls. There is no generic U.N. resolution, or other international guidance, focused on the identification and disruption of proliferation financing as such. The current U.N. framework is based mainly on sanctions against two specific countries (North Korea and Iran) rather than on the threat of financing of proliferation itself.

This focus on country-specific sanctions to control WMD proliferation is an inadequate approach to the problem, for several reasons. First, a better counter-proliferation financing framework could place controls on proliferators where imposing country-specific sanctions is challenging. India's and Pakistan's nuclear programs remain a threat to international peace and stability precisely because the international community failed to agree on sanctions on them. Similarly, the U.N. Security Council was unable to agree on sanctions to control Syria's chemical weapons program. Second, sanctions on North Korea appear to have failed. The economic strain from sanctions has not delayed or deterred the Kim regime from pursuing ever more sophisticated weapons technology. Third, although some states have export controls in place to prevent procurement by, for example, Indian or Pakistani agents, these controls focus on transfers of goods and materials rather than on their financing. Furthermore, no guidance on FoP is available from multilateral export control regimes, informal groups of supplier countries focused on improving export controls, such as the Nuclear Suppliers Group or the Australia Group (though they may be considering the matter).

Several issues complicate the ability of both national authorities and banks to identify financing of proliferation and contribute to the lack of strategy in response. Publicly available information about what financing of proliferation looks like is limited. For example, FoP is regarded by U.S. authorities as a money laundering activity, and proliferation finance typologies are not specifically identified among other money laundering typologies in the U.S. standard banking-sector regulatory supervisory handbook, the Federal Financial Institutions Examination Council.[2]

Identifying FoP on the basis of goods or materials involved is not always reliable. According to data compiled by the U.N. sanctions panel on Iran prior to implementation of the JCPOA, only a small percentage (perhaps 10 percent) of shipments to Iran's nuclear or missile programs included goods and materials listed by multilateral export control regimes as items of specific use in WMD programs.[3] The rest were largely standard industrial items. Their trade was proliferation-related, but their financing appeared legitimate.

The financial signature or trail of a proliferation program may be a way for government investigators, banks, or trade professionals to recognize a proliferator and act to halt or disrupt its activities.

The relative scale of the proliferation threat is also difficult to assess. Compared to the millions of trade-related financial transactions conducted each day by financial institutions, the number of financing of proliferation-related transactions is almost certainly small. Identifying these transactions is akin to looking for needles in haystacks. The U.S. Treasury Department has determined that "deceptive practices have allowed millions of U.S. dollars of DPRK illicit activity to flow through U.S. correspondent accounts,"[4] but no regulators from other countries have attempted equivalent estimates of the scale of financing of proliferation. They almost certainly do not know. The great majority of regulators require no reporting from banks on financing of proliferation as such. So, most FIs do not report financing of proliferation – even if they could identify it, which many cannot (particularly at smaller regional banks).[5] There is very little evidence that financial institutions, apart from, possibly, a few big international banks, have incorporated financing of proliferation indicators into their due-diligence procedures.

Proliferation finance also has received less attention than other illicit finance threats. The FATF published a proliferation financing typologies report in 2008, but since then it has spent much less time on the threat of proliferation financing than on the threat of money laundering and terrorist financing. FATF President Juan Manuel Vega-Serrano told the Security Council in December 2016 that "Financing is an essential component of proliferation. Therefore, financial measures are one of the most effective tools to counter proliferation."[6] Incongruently, however, only two of forty FATF Standards published in 2012 address the FoP threat. Also, the approach to risk is different: Although FATF Standards require countries to take a risk-based approach to money laundering and terrorist financing, the approach to FoP remains rule-based and narrowly focused on targeted financial sanctions. The grave security concerns about the insidious and dynamic nature of proliferation dictate a wider and risk-based approach instead. (See FATF Recommendations below).

There is very little evidence that financial institutions have incorporated financing of proliferation indicators into their due diligence procedures.

Perhaps taking their lead from FATF, most financial authorities also pay less attention to it than money laundering or terrorist financing. This is a mistake. The disruption to the international financial system from an event involving WMD – for example, the launch of a North Korean nuclear-tipped ballistic missile – is likely to be catastrophic. That threat is coming closer: U.S. intelligence assessments have apparently concluded that North Korea will be able to produce a "reliable, nuclear-capable ICBM" program sometime in 2018.[7]

As a final reason explaining the lack of effort to counter FoP, for most authorities, countering WMD proliferation involves actions to stop goods and materials, usually by means of licensing or export controls, or interdictions. Such actions might be easier to identify, and success easier to quantify, than actions against financial networks.

Understanding Financing of Proliferation: A Model

A state intent on acquiring WMD probably will take the decision to do so in secret. Construction of program infrastructure, and procurement of needed goods and materials, will be carried out covertly, at least until the state feels sufficiently secure or the WMD program is discovered by the international community. At that point the U.N. Security Council might impose sanctions, or if not, other measures such as unilateral sanctions might be put in place (perhaps by the European Union [EU], United States, or other countries), or controls on exports of materials and technology needed by the programs.

All WMD programs therefore aspire to financial self-sufficiency to shield themselves from such controls, and the more mature and established WMD programs (such as India's or Pakistan's) are likely to be largely although not completely domestically self-sufficient. Less mature or new WMD programs will be more dependent on procurement of goods and materials from overseas. Financial characteristics of WMD programs therefore will largely reflect two considerations. The first is maturity; are the programs mature and self-sufficient, in which case the bulk of costs will be in-country program support (such as for infrastructure, administration and salaries)? Or are they less mature, in which case costs of overseas procurement (for example goods and materials, payments to procurement agents) will be a larger proportion of overall costs? The second consideration is whether international sanctions, or national sanctions or export controls, have been imposed. Where this is the case, proliferating networks have to be adept at hiding their sources of funds, as well as the end-users and end-uses of goods and materials they are trying to procure.

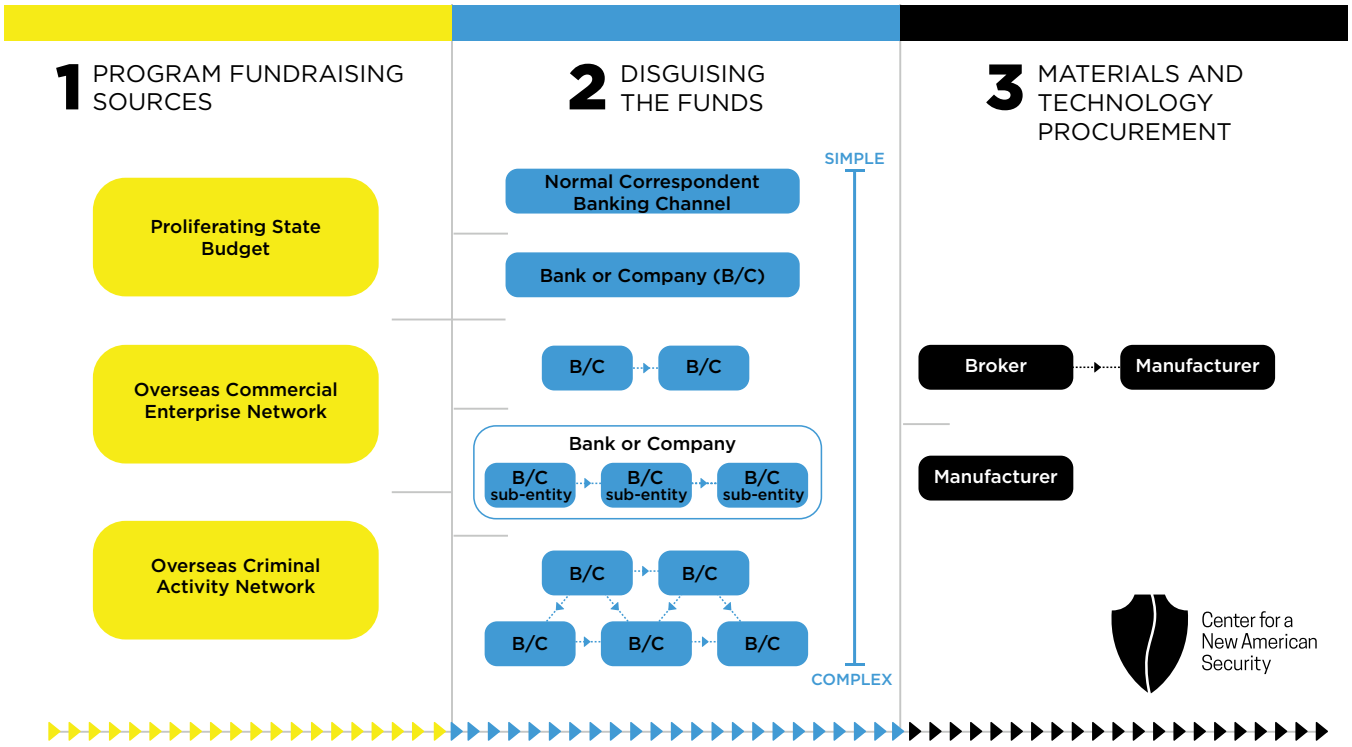
The financial elements of a WMD program can be broken down into three stages (as depicted in Figure 1: Three stages of FoP):

- "Program fundraising": A proliferating country raises financial resources for in-country costs.
- "Disguising the funds": The proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes.
- "Materials and technology procurement": The proliferating state or its agents uses these resources for procurement of materials and technology within the international financial system.

It may be tempting to equate these three stages of FoP to stages in money laundering. For example, there are some similarities between the "placement" and "layering" of illicit funds into the financial system to disguise detection, and "disguising the funds."

Such a parallel, however, is inexact. Money launderers engage in a circular process. They take criminally generated illicit funds, launder them, and make them available to themselves again in licit form. The financing of proliferation is, instead, a linear process. Proliferators move illicit funds through the stages and use them to pay reputable industrial manufacturers for goods and services.

Figure 1. Three stages of FoP



The diagram is simplified and, for example, does not include the financing of shipments of procured goods and materials to their end-users. The form of transactions that constitute "disguising the funds" will depend on how extensive the financial sanctions are that they are trying to circumvent.

The majority of financial transactions of mature state-sponsored WMD programs will fall into the stage of "program fundraising." Funds will be allocated from departmental budgets, but if these are tight due to sanctions, proliferating states might try to supplement them with profits from trading carried out by overseas procurement networks (in the case of North Korea). Although to date there is no publicly available evidence of such activity, it is possible that funding for WMD programs also might be supplemented by proceeds of criminal activity (for example, in the case of Iran, embezzlement of Central Bank of Iran funds held overseas[8]) or by proceeds from cyber theft or attack.[9]

Only local banks or financial institutions are likely to be involved in program fundraising activities. International financial institutions probably will not hold information relating to such activity in their databases unless they have correspondent relationships with these local banks. Information about program fundraising activities most likely will be accessible to intelligence or law enforcement agencies, who are likely to keep mature proliferation states under scrutiny because of the threat they represent to international peace and security.

In the absence of financial sanctions, the second stage (disguising the funds), the movement of assets into the international financial system for trade purposes (often involving a foreign exchange transaction), probably would consist largely of straightforward transfers between local banks and counterparts overseas, including international financial institutions. In the presence of U.N., U.S., or EU financial sanctions, particularly if the proliferating country's banking system is significantly cut off (as was the case with Iran and is now the case with North Korea), the disguising of funds will be a major challenge for proliferating states. It would involve circumvention of financial sanctions and could take the form of cash deposits to banks or money service businesses in neighboring countries (perhaps in less regulated jurisdictions) or *hawala* transactions. Front companies overseas may act as money remittance businesses (probably unlicensed) on behalf of sanctioned entities or may carry out business on behalf of each other in order to minimize movement of money between them. Ledger systems may be used to keep accounts.[10]

Global banks will be involved in international disguising of funds although transactions will be difficult to identify because of the complex networks of procurement agents and front companies involved. Open source information about disguising the funds may include records of prosecutions of sanctioned entities or unlicensed money-remittance businesses, such as cases in Sweden, Singapore, and the United States.[11] Government authorities may publish information on individuals or entities, or sanction-circumvention techniques,[12] or may share information privately with select institutions.

The procurement of materials and technology stage involves international financial system transactions to pay for goods and materials, either directly to manufacturers, or more likely via brokers or trading companies. Where possible, procurement networks seek high-quality goods and materials from reputable manufacturers. These manufacturers in turn will seek guarantees that the business is legitimate and will expect to be paid through conventional channels involving reputable financial institutions. Payments for shipping and transport of materials and technology also will fall into this final category of proliferation-related money transfer.

The procurement of materials and technology stage involves international financial system transactions to pay for goods and materials, either directly to manufacturers, or more likely via brokers or trading companies.

A large proportion of the financing of new or immature WMD programs will fall into the category of procurement of materials and technology. Financial institutions will be fully involved, although the transactions themselves will be difficult for banks and brokers to identify because they resemble legitimate trade of industrial items. Information about activities falling into the procurement of materials and technology stage can be found in court cases involving sanctioned entities or unlicensed money-remittance businesses. Government authorities may share information on individuals or entities involved, or on circumvention techniques. Banks also may recognize the signature of proliferation activity and agents in their financial databases.

Recognizing Proliferation Finance: Typologies and Observations

It is difficult to translate a theoretical understanding of how proliferators move and use their money to build weapon programs into an ability to recognize its signatures in the real world. Publicly available material about the characteristics of FoP, or documented methodologies, has been relatively sparse. The FATF report of 2008 included case studies and a list of 20 possible indicators (although, as the report points out, many were possible indicators of other types of trade-based financial crime).[13] U.N. Expert Panel reports relating to Iran and North Korea include additional case studies.[14] U.S. law enforcement documents also can include relevant information,[15] as do court records from other jurisdictions, such as Sweden and Singapore. However, very few scholars or compliance professionals have the time and resources to methodically comb through these disparate sources of data to bring together a consolidated set of examples.

The Project Alpha report compiles and analyzes much of this information, together with new data provided by national authorities and financial institutions. It is intended to act as a guide for government authorities to enhance identification of financing of proliferation and to expand the guidance they provide to financial institutions. It is also intended to help the financial sector identify financing of proliferation and better inform national governments (ideally global institutions would set reporting standards in this respect). Notably, the report modifies and updates the FATF's 20 possible indicators (Project Alpha Indicators of Possible Financing of Proliferation are summarized in the Box: Indicators of Possible Financing of Proliferation[16]). The great majority of cases described in the report contain elements that fall into the procurement of materials and technology stage of Figure 1. Of these, perhaps 40 percent also contain elements that can be described as transactions that proliferators use to disguise their money and enter opaquely into the international financial system (disguising the funds). Less than 1 percent of the cases cover activities by proliferator states to raise the money they plan to use for advancing their WMD programs (program fund-raising).

Overall, the report paints a picture of a variety of mechanisms by which states finance proliferation to build and maintain WMD programs, and how these can adapt to circumvent sanctions or other controls. Even accounting for variations in quality and quantity of data, the report provides crucial insights into differences between the networks supporting North Korea and Iran, and perhaps Syria, and those supporting the WMD programs of Pakistan and India. With such insights public policymakers and financial institutions can develop better strategies to counter WMD security threats.

> **Following financial sanctions imposed by the United Nations, United States, and the European Union, the DPRK set up an extensive and sophisticated network to circumvent these measures.**

For example, following highly restrictive financial sanctions imposed by the United Nations, United States, and the European Union, North Korea set up extensive and sophisticated networks to circumvent these measures, involving companies and banks overseas, usually in China but also elsewhere in East and Southeast Asia. These networks enable North Korea to procure goods and materials for its nuclear and other WMD and missile programs from a range of suppliers, and to maintain access to the international financial system in order to pay for them. The networks may trade a variety of goods and materials in addition to WMD-related items, and may be self-financing. Companies may act as money remittance businesses. Some elements may have connections to North Korean diplomatic missions. As an example of these kinds of transactions, Figure 2: North Korea's Procurement Networks demonstrates the connections identified by the UN Panel of Experts on North Korea between North Korean proliferation networks and front companies based in China, Malaysia, Hong Kong, and the Middle East, set up by the North Korean company Pan Systems Pyongyang.

Indicators of Possible Financing of Proliferation[42]

ELEMENTS OF TRADE-RELATED TRANSACTIONS POTENTIALLY HIGHLY INDICATIVE OF FOP

- Parties are physically located in proliferating countries
- Parties are physically located in countries of diversion concern (states that allow the provision of proliferation-sensitive goods, or their financing, through their territory)
- Details of parties are similar to parties listed under WMD sanctions or trade controls (for example, names, addresses, or telephone numbers)
- Parties are conducting business in goods and/or technology controlled on WMD grounds
- Parties involved conduct business activity inconsistent with their profile
- End-user not identified
- Parties maintain connections with a country of proliferation concern
- Goods ordered from third countries
- Cash used in transactions for industrial items
- Highly technical goods shipped to countries with low levels of technology

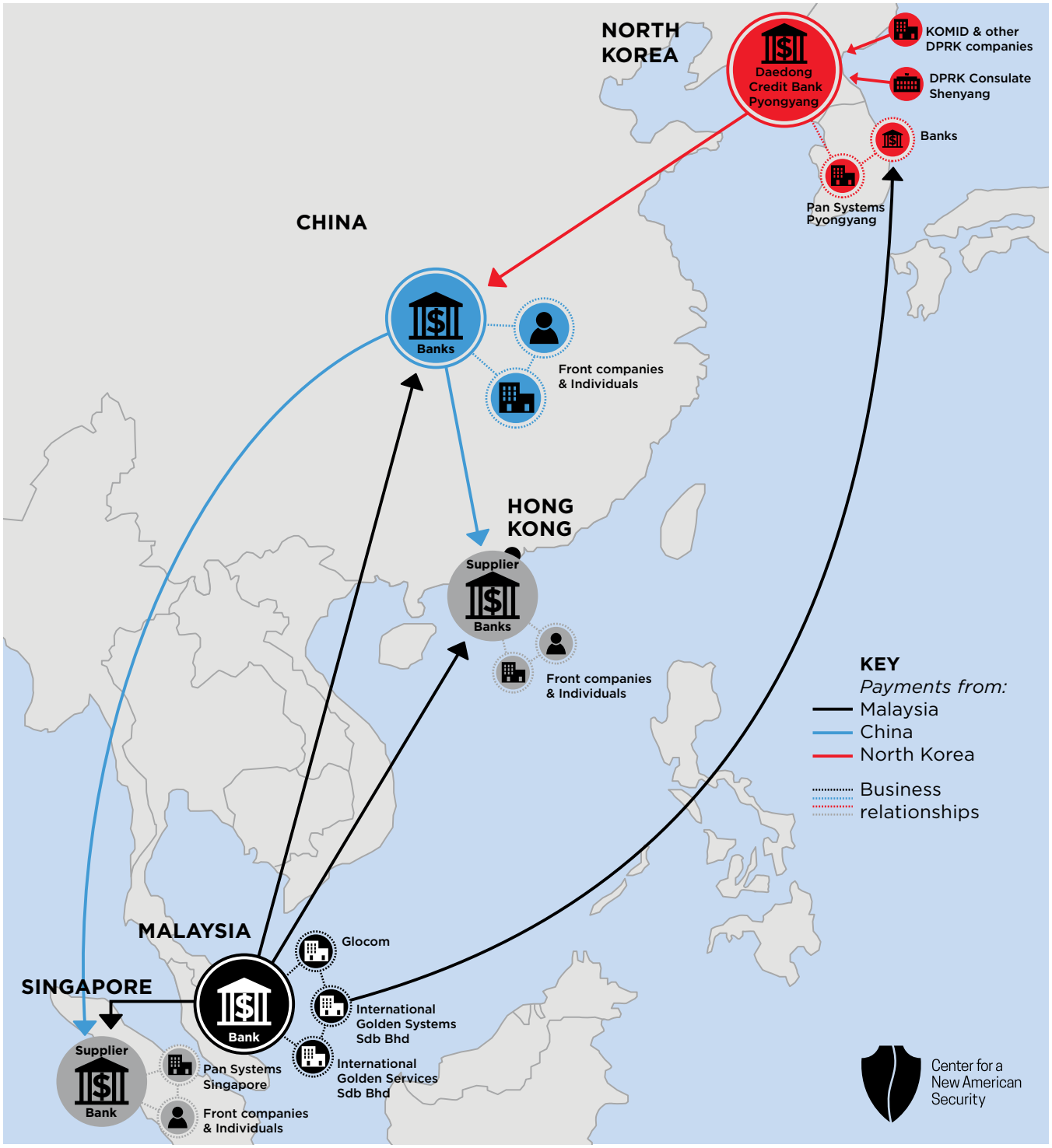
ELEMENTS OF TRADE-RELATED TRANSACTIONS POTENTIALLY MODERATELY INDICATIVE OF FOP

- Parties are organized in a way that is highly suggestive of front or shell companies
- Parties do business as small trading, brokering, or intermediary companies
- Parties conduct trade in export-controlled products
- Commercial business is acting as money-remittance business
- Transactions are completed on the basis of "ledger" arrangements
- Parties to financial transactions are linked (for example, common physical address, IP address, telephone number, or their activities are coordinated)
- Parties exchanging goods are linked (for example, common ownership or management)
- Parties maintain links to a university in a proliferating country
- Parties provide trading documentation with non-specific or misleading descriptions of goods
- Parties provide documents that are fake or fraudulent
- Personal accounts are used to purchase industrial items
- Parties conduct business with financial institutions with weak anti-money laundering/countering terrorist financing controls; or in countries with weak export control laws
- Parties use circuitous routes of shipments or circuitous routes of financial transactions
- Shipment of goods is inconsistent with normal trade patterns
- Trade finance transaction involves shipment through country with weak export control laws or their enforcement
- Parties are located in countries with weak export control laws or their enforcement

ELEMENTS OF TRADE-RELATED TRANSACTIONS POTENTIALLY WEAKLY INDICATIVE OF FOP

- Declared value of shipment is obviously undervalued
- Customer provides inconsistent information in trade documents and financial flows
- Customer conducts unusual pattern of wire transfers for no apparent purpose
- Customer provides incomplete information
- New customer requests letter of credit transaction while awaiting approval of new account
- Payments connected with parties not identified on original letter of credit or other documentation

Figure 2: North Korea's Procurement Networks

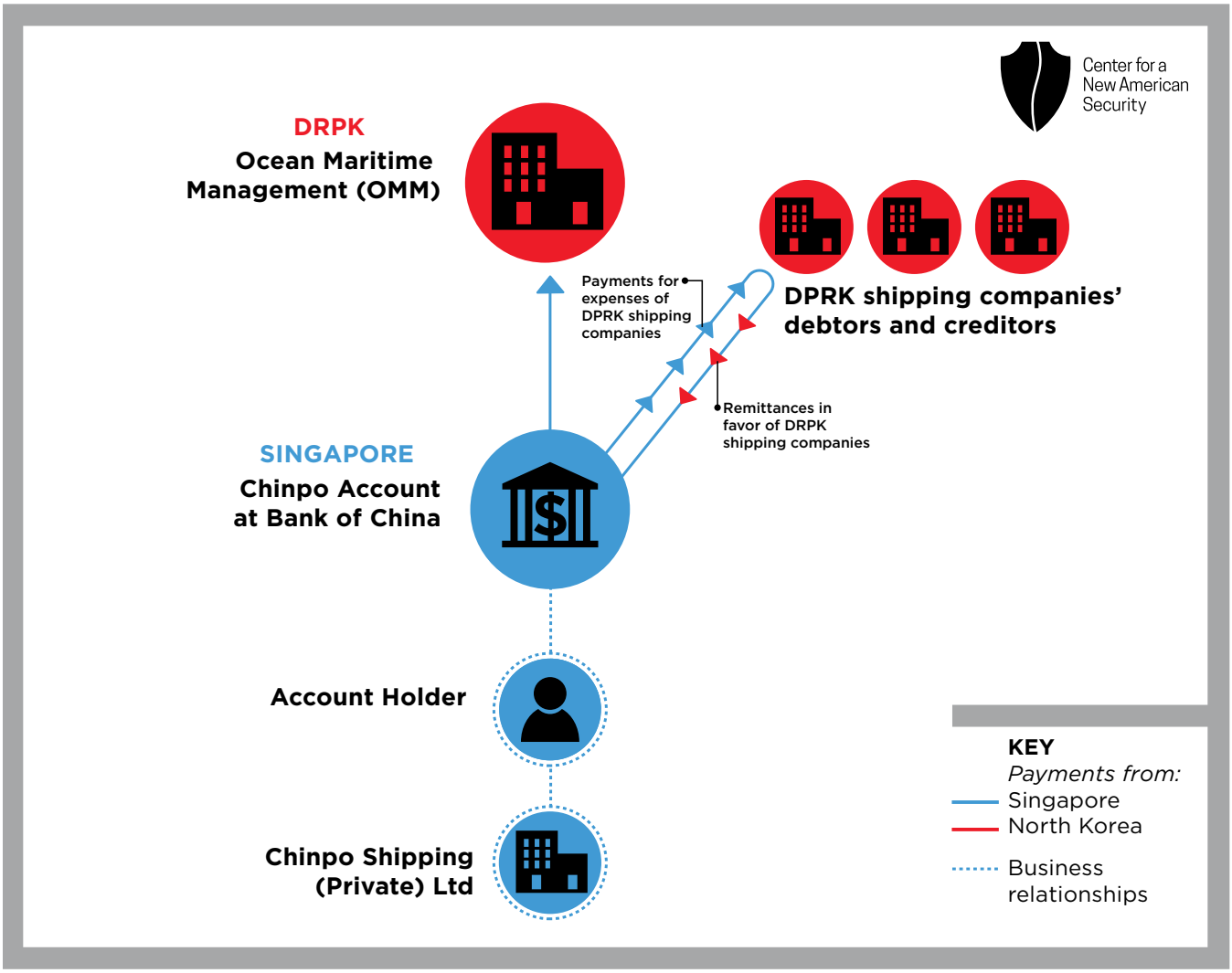


A simplified illustration of North Korea's sophisticated procurement networks, based in multiple countries. In this particular case, Pan Systems Pyongyang and its front companies carry out financial activity in multiple jurisdictions, which benefits, among others, the Korea Mining and Development Trading Corporation (KOMID), widely considered to be North Korea's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. Pan Systems Pyongyang's involvement in Middle East business is referenced without details (not shown). Figure based on Project Alpha Report on Typologies of Financing of Proliferation, October 2017, which is based on the 2017 Final Report of the UN Panel of Experts on DPRK.[43]

North Korean shipping companies play a major role in the circumvention of sanctions. They transport prohibited materials for North Korea's nuclear and other WMD programs from major ports in Southeast Asia and beyond, and they serve as a source of income. But their access to the international financial system increasingly has been constrained by financial sanctions, and as a result some have relied on foreign companies to act as bankers. One such Singaporean company, a shipping agent, was prosecuted by its national authorities for processing financial transactions on behalf of a North Korean shipping company through an account at the Bank of China (Figure 3: Chinpo Shipping Case Study).

One concerning characteristic of current proliferation finance activity is that several of the networks continued to operate despite evidence that the authorities know of their activities.

Figure 3: Chinpo Shipping Case Study



Chinpo Shipping (Private) Ltd., a ship's agent based in Singapore, acted as an unlicensed money remittance business on behalf of Ocean Maritime Management, a DPRK shipping company and other DPRK shipping companies (figure based on Project Alpha report on Typologies of Financing of WMD Proliferation, October 13, 2017, in turn based on a report by the UN Panel of Experts on DPRK).[43]

Although data on the networks that finance the Pakistani and Indian WMD programs are very limited in comparison with those of North Korea and Iran, they suggest that networks supporting WMD spending of India and Pakistan are relatively simple. For example, the data show relatively few front companies involved, and there are no examples of companies acting as money remittance businesses. These characteristics may reflect the greater ease in conducting illicit proliferation by India and Pakistan given that they are not subject to U.N. or unilateral financial sanctions. Additionally, unlike the North Korea – or Iran-focused sanctions programs, the coercive economic measures directed against India and Pakistan are relatively limited, and were implemented too late to prevent either country from compiling the know-how and technology for sophisticated WMD programs.[17] Although many states have export controls in place, they are focused on preventing transfers of goods and materials to India's and Pakistan's WMD programs, rather than on their financing. Professionals in global banks and companies have little requirement or incentive to be on the lookout for Pakistani or Indian proliferation.

In the presence of sanctions, networks must evolve. For example, the Syrian Scientific Studies and Research Center (SSRC),[18] thought to be the main body developing Syria's chemical weapons and ballistic missile programs, conducted procurement before 2011 by negotiating and ordering goods from

In the presence of sanctions, networks must evolve.

foreign suppliers through front companies. The front companies made corresponding payments separately, through companies based in tax havens and offshore financial centers funded by wire transfers from the SSRC. Following U.S. and EU sanctions on many of the front companies, the SSRC turned to Syrian businessmen who were funded in cash to carry out SSRC procurement. In 2014 and 2015, following further international sanctions, the SSRC worked to shield itself by directing Syrian businessmen to evade sanctions by extending existing overseas business networks, particularly to exploit Chinese suppliers.

Proliferators may now make less use of trade finance than they once did, which is significant for efforts to track FoP. More than half of the case studies in FATF's 2008 report on proliferation finance typologies involved letters of credit, but these constituted only a small minority of cases in the Project Alpha study. While in some cases Iran's proliferation program used trade finance, none of the North Korean cases did so. This shift may reflect decreasing use of letters of credit in international trade generally,[19] or even inadequate data, but it also may reflect conscious decisions by proliferators to avoid using trade finance. Although trade finance represents only about 20 percent of global trade,[20] it is based on checkable documentary information and offers more opportunities for due diligence than does the alternative payment mechanism, open account transactions (wire transfers based on direct agreements between buyers and sellers).[21] Open account transactions provide financial institutions with very limited information against which to screen or monitor for indicators of FoP or other financial crime.

To date, proliferators continue to use established financial mechanisms – wire transfers, trade finance products, cash, checks, and, in a few cases, credit cards. There are no FoP examples involving virtual currencies or new payment methods. It is possible that proliferators using virtual currencies may have avoided detection, and that proliferation finance in such currencies is particularly difficult to spot. Law enforcement officials or regulators may need to access records that are masked by anonymous features of virtual currencies, or distributed across various jurisdictions, perhaps including jurisdictions with weak anti-money laundering/countering terrorist financing regimes.[22] But it is more likely that, as in the case of using these new technologies for terrorist financing, so long as classic and established financial mechanisms of evading sanctions are still accessible there is probably no need to invest in new techniques to transfer payments that may feature a greater barrier to entry. Nevertheless, commercial enterprises are looking to utilize virtual currency technology for legitimate trade purposes,[23] and virtual currencies offer opportunities for cybercrime that could extend to financing of proliferation in future.

One of the particularly concerning characteristics of current proliferation finance activity is that several of the networks continued to operate despite evidence that the authorities know of their activities and in some cases have taken action against them. Whether for reasons of ideology or profit, the individuals involved were persistent, and managed to set up resilient networks able to adapt and continue activities despite pressure from authorities.

Inadequate International Controls, Inadequately Implemented

The relative paucity of international controls on FoP is exacerbated by failure on the part of many countries to implement them effectively. The problem starts with the U.N. Security Council resolution that underpins the control framework, Resolution 1540 (2004), approved by the Security Council in response to the threat from state-sponsored proliferators (exemplified by the nuclear-smuggling mastermind, Pakistan-based Abdul Qadeer Khan and his proliferation network) and from terrorists.

Resolution 1540 (2004) places obligations on all U.N. member-states, and implementation is encouraged through "dialogue, outreach assistance and cooperation."[24] It includes just two references to FoP, in the form of requirements to implement controls to prevent financing of WMD activities by terrorists and financing of WMD-related exports, with nothing further specified. Despite the lengthy amount of time the resolution has been in force, it is clear that many states have yet to implement these fundamental measures. According to a mid-2016 review, few states had "dedicated separate proliferation financing legislation" although "good progress [had] been made to prohibit the financing of proliferation activities and enforce such prohibitions."[25] Perhaps in acknowledgement of the difficulties U.N. member states have encountered, successor Resolution 2325 (2016) directs the 1540 Committee to increase its efforts to support states on financing of proliferation. The Committee will need significant support from member states in doing so.

The relative paucity of international controls on FoP is exacerbated by failure on the part of many countries to implement them effectively.

In contrast to the rather general terms in which financial requirements are set out in Resolution 1540 (2004), the series of Security Council sanctions on North Korea's WMD programs, and on Iran prior to the JCPOA, make relatively specific financial demands (although with no reference to FoP as such). These include a mixture of targeted financial sanctions (requiring assets of listed parties to be frozen), activity-based sanctions (prohibiting financing of certain activities), sectoral sanctions (focused on particular economic activities, although these did not feature in Iran sanctions),[26] and other financial measures.[27] They effectively prohibit a large proportion of financing associated directly or indirectly with FoP in these two countries. States that have mechanisms in place to implement financial sanctions on North Korea and Iran are well placed to implement the financial requirements of Resolution 1540 (2004).

In the case of Iran, U.N. financial sanctions, complemented by U.S. and EU measures that effectively choked off Iran's oil and gas industry, were fundamentally important to securing the JCPOA in July 2015. In the case of North Korea, however, despite increasingly restrictive U.N., U.S., and EU financial measures over the last several years, the country's leadership has yet to come to the negotiating table. The increasing scope of U.N. financial sanctions over this period is instructive, despite their failure to produce diplomacy: In 2009, they consisted of asset freezes on just five individuals and eight entities. As of December 2017, U.N. member states are required to implement a far wider range of financial sanctions including:

- Freezing assets of 79 individuals and 54 entities listed by the U.N. Security Council, and of entities of the North Korean government and the Korean Workers' Party (if involved in prohibited activities).
- Prohibiting any provision of financial services or assistance related to North Korea's prohibited programs, or evasion of sanctions, including bulk cash and gold (the requirement extends to companies that might perform financial services normally provided by banks).
- Ceasing any business involving North Korean banks in their territories, and any business involving their own banks in the North Korea, and any financial support (including insurance) for trade with North Korea.
- Banning any procurement by DPRK of industrial machinery, transportation vehicles, iron, steel and other metals, condensates and natural gas, and limits procurement by DPRK of crude oil and refined petroleum products.

Banning any export by DPRK of food and agricultural products, machinery, textiles, coal and iron ore, seafoods, and other products and metals.

Why are the outcomes of these two financial sanctions regimes so different? One reason may be that unlike Iran, North Korea has a higher tolerance for the economic pain that it inflicts on its citizenry. North Korea is also

not a regional economic center with a history of trading relations with the rest of the world. As the Trump administration has charged, Chinese companies are standing in the way of full compliance, making North Korea inherently less vulnerable to economic or financial pressure.

A second possible reason is that U.N. sanctions have been applied incrementally over more than ten years, and North Korea has invested heavily in the illicit networks necessary to evade them. The financial measures currently in place constitute what is effectively a U.N.-mandated trade embargo on North Korea. Had this approach been implemented from the start, rather than a loosely applied set of narrower sanctions focusing only on North Korean agencies procuring missile and nuclear equipment and technology, financial sanctions could have been more successful in changing North Korea's WMD policy.

The third reason is that for U.N. sanctions to be impactful they must be implemented by all states to a uniform high standard, otherwise proliferators will, as they are already doing, exploit weak points. However, many states do not implement U.N. sanctions effectively. This is easily demonstrated: U.N. Security Council sanctions resolutions on Iran and North Korea required states to submit implementation reports. In the case of Iran fewer than half did so,[28] and this is similarly true of North Korean sanctions.[29] Furthermore, many of the North Korean sanctions-implementation reports show that few U.N. member states effectively incorporate the full range of financial sanctions into national legislation (this was also the case with U.N. sanctions on Iran). This means that member states have not passed laws to prosecute the proliferation finance activity banned by the U.N. The implication is that North Korean agents, for example, can function with impunity in their country. The FATF Asia/Pacific Group website offers a good model for legislation, but lack of capacity, apathy, and lack of political will are major barriers to states adopting such legislation.[30]

The absence of formal monitoring of individual states leads directly to the ineffective implementation of financial sanctions and encourages proliferators to act with impunity. U.N. Sanctions Committees do not impose penalties on member states for lax implementation or reporting. The situation is partly mitigated in the case of countries that are members of FATF or of FATF-style regional bodies (FSRBs). FATF and similar organizations can act as motivators, since members of those bodies undergo periodic evaluations of their financial controls, measured against set FATF standards, including implementation of U.N.-targeted financial sanctions on North Korea and on Iran.[31] The FATF evaluations carried out to date provide further evidence that many countries do not implement U.N. financial sanctions effectively. For example, many countries are not able to freeze assets of U.N.-designated individuals or entities "immediately" as required by U.N. resolutions on North Korea,[32] or "without delay" as required by FATF.[33] The requirement usually is interpreted as meaning "within hours," and the ability to take action within this time scale is critically important to the effectiveness of asset-freezing measures so as to prevent the adaptation of proliferation networks.

The absence of formal monitoring of individual states leads directly to the ineffective implementation of financial sanctions and encourages proliferators to act with impunity.

Mitigating the Risk of Financing of Proliferation

The FATF evaluation process is crucial to our understanding of how FATF and FSRB countries implement U.N.-targeted financial sanctions on North Korea and on Iran in practice. However, FATF standards do not extend to the full range of U.N. financial sanctions, including activity-based or sectoral sanctions, and so countries are not evaluated on their implementation of these. This situation represents a major gap in FATF's coverage of FoP, but there are others.

FATF Recommendations

The work of FATF is key to ensuring the integrity of the global financial system. The organization is the global standard-setter for money laundering, countering the financing of terrorism, and countering proliferation finance. FATF published a list of 40 recommendations in 2012 that serve as model policies in these fields. In addition to creating policy guidance, FATF also tracks the implementation of its standards through the Mutual Evaluation Reviews it conducts for its members.

The recommendations also offer potential elements of a framework to counter proliferation financing. Unfortunately, however, only two of the 40 recommendations refer to the proliferation finance threat. These are Recommendation 7 (covering U.N.-targeted financial sanctions relating to proliferation) and Recommendation 2 (relating to national cooperation and coordination).

The other FATF recommendations are drafted with no reference to FoP, yet many of them also are very important to countering FoP. For example, Recommendation 1 requires risk-based approaches to countering money laundering and terrorist financing threats. A risk-based approach means proactively assessing, evaluating, and monitoring the risk to which institutions and countries are exposed and taking the necessary mitigating actions. Recommendation 1 does not extend to FoP. It should do so.

Recommendation 40 calls for international cooperation on exchanges of information with foreign partners. These efforts are critical to strengthening the international framework for identifying and countering proliferation financing, yet FATF does not specify the FoP threat in this recommendation. It should do so.

None of the following further FATF recommendations refer to the FoP threat, but they should, because by implementing them countries would further strengthen their defenses against the FoP threat:

- Customer due diligence (CDD, Recommendation 10): The requirement should be extended to ensure that CDD procedures reflect the FoP risk.
- Correspondent banking (Recommendation 13): The requirement should ensure that correspondent banking due diligence standards extend to FoP.
- Money transfer services (Recommendation 14): The requirement should be updated to ensure that due diligence extends to the FoP risk.
- Wire transfers (Recommendation 16): The requirement should ensure that documentation requirements reflect FoP requirements.
- Internal controls/foreign subsidiaries (Recommendation 18): The requirement should ensure that company procedures reflect FoP risk.
- Higher-risk countries (Recommendation 19): The requirement should ensure that provisions to deal with higher-risk countries take account of FoP risk.
- Reporting of suspicious transactions (Recommendation 20): The requirement should be extended to FoP risk.
- Transparency/Beneficial ownership (Recommendation 24): The requirement should reflect FoP risk.
- Regulation and supervision (Recommendation 26): The requirement should extend to FoP risk.
- Powers of supervisors (Recommendation 27): The requirement should ensure that responsibilities include FoP.
- Financial intelligence units (Recommendation 29): The requirement should be extended to FoP.
- Legal responsibilities (Recommendation 30): The requirement should be extended to FoP.
- Cash couriers (Recommendation 32): Requirements should be extended to FoP risk.

U.S. Tools for Countering Proliferation Finance

The United States is the only country evaluated by FATF to date that has a robust set of financial measures in place requiring banks and companies to identify and impede the financing of proliferation. This is the driver behind successful use of criminal cases and civil asset forfeitures to go after proliferators in recent years (see Box: U.S. Tools for Countering Proliferation Finance).[34]

In their fight against illicit financial flows, U.S. officials have developed a diverse suite of legal tools and authorities. They can use them to expose and counter the financing of proliferation. These include:

- Criminal indictments and civil asset forfeiture
- Requirements for financial institutions to file Suspicious Activity Reports, Currency Transaction Reports, and other documents required by the Banking Secrecy Act
- Section 311 of the USA Patriot Act – to block correspondent accounts, obtain information, designate parties of primary money-laundering concern
- Section 314(a) of the USA Patriot Act – Enables law enforcement to communicate queries to financial institutions
- Section 314(b) of the USA Patriot Act – enables financial institutions to share information
- Geographical Targeting Orders
- Reports on Foreign Financial Agency Transactions
- Demand letters – for required records of insured depository institutions
- FinCEN and other law enforcement advisories – can identify red flags and typologies
- Sharing of information with foreign Financial Intelligence Units.

In addition to instituting an adequate legislative framework, policymakers should ensure that other key elements of an appropriate counter–proliferation finance effort are in place. First, national authorities must learn how to conduct financing of proliferation risk assessments. This is especially important because risk assessments are not U.N. or FATF requirements. As a result, few authorities have carried out a FoP risk assessment. As demonstrated by U.N. Panels on North Korea and on Iran, it is incumbent on nation-states to understand the sophisticated global reach of attempts to circumvent financial sanctions.[35] In the absence of a risk assessment, national authorities have no basis to conclude that their financial systems are at any less or greater risk of FoP than others. Some elements of a basic FoP risk assessment are listed in the box: Designing a FoP Risk Assessment.

Second, to maximize the effectiveness of efforts to counter FoP it is vital that government departments and agencies should ensure proper channels of communication and coordination.[36] These should include the following sources of subject matter expertise:

- Export control and licensing authorities, and customs agencies
- Ministries of Finance, Economy, and Commerce, which are responsible for financial aspects of trade
- Financial intelligence units, and defense, intelligence, and security services, which maintain sophisticated network analysis and data collection competencies.

To maximize the impact of international efforts to counter FoP it also is vital for international partners to have effective channels of communication.[37] Information is most likely to be exchanged between FIUs (perhaps on Egmont Group channels) or intelligence agencies. Foreign intelligence material (possibly highly classified) may be important to identifying and combating FoP, given the complexity of networks and the difficulty of their identification.

Third, financial institutions potentially play a key role in countering financing of proliferation because they will be involved in processing many of the purchase transactions for WMD equipment and materials, and their financial records may include FoP-relevant information. It is critically important for legal compliance and reputational protection that, on the basis of risk assessments, financial institutions take appropriate measures to identify financing of proliferation, and that they report suspected proliferation finance activity in suspicious transaction or suspicious activity reports (STRs/SARs). Ideally these reports should carry a FoP label because this will help public authorities know when banks are seeing proliferation finance activity, and facilitate the decisions authorities will need to make over investigative priorities and resources. Perhaps as important, labeling STRs as financing of proliferation also will ensure better statistics are collected about the scale of the FoP threat, and contribute to understanding the structure of proliferating networks.[38] In a virtuous circle, better statistics will ensure that national authorities and FIs conduct better risk assessments.

Designing a FoP Risk Assessment

In order to mitigate financial threats, countries and financial institutions need to understand their financial risks. Conducting formal financial risk assessments is crucial, and these assessments underpin FATF standards. For financial institutions, risk assessments usually are based on considerations of geographical location, business processes, and customer base. The following factors may be relevant to formulating a risk assessment of proliferation financing.[39] The list is not intended to be comprehensive, and national authorities or financial institutions can adapt these factors to meet the specific circumstances in which they operate. Furthermore, financial institutions may need to match their own business model with these factors, and weigh them in proportion to their own experience with customers.

GEOGRAPHICAL RISK FACTORS

- Commercial or business ties, or financial relationships (such as correspondent banking relationships) with a country that is subject to U.N. sanctions imposing WMD-related restrictions (North Korea, Iran, for example), or to unilateral sanctions (Syria, for example), or in their neighborhood
- Commercial or business ties, or financial relationships (such as correspondent banking relationships) in countries with diplomatic, trade, or corporate links to states of proliferation concern or in their neighborhood (for example, China, Singapore, Malaysia, United Arab Emirates, or Turkey)
- Links (such as funding or other support) with WMD proliferation activities, such as those identified by the U.S. Department of the Treasury (Office of Foreign Assets Control); the EU or national authorities such as the United Kingdom.

CUSTOMER RISK FACTORS

Categories of customers whose activities may indicate a higher risk include, but are not limited to:

- Those on national lists concerning WMD proliferation
- Military or research body connected with a higher-risk jurisdiction of proliferation concern
- Customer or counter-party involved in the manufacture, supply, purchase, or sale of dual-use, proliferation-sensitive or military goods
- Customer who is a small trader/intermediary, may be dual-national of country of proliferation concern
- Customer located in a major financial or trade center.

PRODUCT AND SERVICE RISK FACTORS

The following list of possible risks is not exhaustive:

- Delivery of services possibly subject to sanctions, e.g. correspondent banking services (subject to U.N. North Korean sanctions)
- Project financing of sensitive industries in jurisdictions of proliferation concern
- Trade finance services, transactions, and insurance products involving jurisdictions of proliferation concern
- Transfer of dual-use, proliferation-sensitive goods and materials to a country of diversion concern.

Lessons to Counter Future WMD Proliferation

It is possible to predict financing of proliferation signatures of future possible illicit WMD programs. For example, industrially developed countries seeking a covert WMD program will have relatively little need for overseas procurement, and if they have sophisticated financial systems it will be relatively easy to hide proliferation finance.

Countries with highly developed industries will probably be able to manufacture many WMD components themselves and would not need large overseas procurement programs. If they already possess civil nuclear facilities they might not need to procure fissile material (although diversion of such material would become apparent during inspections by the International Atomic Energy Agency).

The FoP signatures of such WMD programs would fall primarily into program fundraising. They would look similar to FoP signatures of mature WMD programs. Information on such FoP would probably would be available mainly to national intelligence agencies. Local banks or other financial institutions may be involved in program fundraising activities, but unless correspondent relationships exist, international financial institutions are unlikely to process proliferation-related transactions and unlikely to hold information on proliferation finance in their databases for such activities.

In contrast, countries intent on developing a nuclear or other WMD program, but lacking a strong industrial base, would largely depend on overseas procurement of necessary goods and materials. FoP signatures would fall largely into disguising the funds and purchase of proliferation goods and technology, and international banks may well be involved in financial transactions.

Ultimately, how a state transfers funds through the international financial system will depend on the sophistication of its financial infrastructure, especially its connections to international financial institutions. Nuclear or other WMD programs under heavy financial sanctions would need to find creative ways to transfer funds into the international financial system. The presence of a large and sophisticated banking sector would facilitate transfer of illicit funds into the global financial system. Otherwise, cash deposits and informal mechanisms such as *hawala* transfers probably would be involved. Commercial or financial entities also may need to establish partnerships with companies located outside sanctioned jurisdictions that are prepared to conduct financial transactions on their behalf. The FoP signatures of such programs would fall into the disguising the funds and procurement of materials and technology stages of FoP.

WMD programs that are not subject to financial sanctions will not need to develop sophisticated circumvention mechanisms. Overseas networks may not need to be elaborate, as appears to be the case (based on the limited information available) with Pakistan's and India's WMD programs.

To date, proliferation networks exclusively have used established financial mechanisms including wire transfers, trade finance products, cash, and checks, suggesting they do not need more sophisticated and anonymous financial payment mechanisms. If a rogue state developed a covert WMD program in the next five to ten years, it is likely that its financing of proliferation signatures would follow the classic patterns. Nevertheless, if proliferators were considering the use of new payment methods such as virtual currencies, the size and sophistication of the financial sector in which they were operating might be a determinant. Financing of proliferation involving virtual currencies probably would fall into primarily into program fundraising or disguising of funds, but if industrial manufacturers started to receive payment using virtual currencies then transactions could fall into the stage of procurement of proliferation materials and technology.

> **Countries intent on developing a nuclear or other WMD program, but lacking a strong industrial base, would largely depend on overseas procurement of necessary goods and materials.**

This analysis of FoP signatures of possible future WMD programs will assist policymakers crafting new sanctions or other controls to target proliferators. For example, to shut down overseas procurement networks, particularly those of new or immature WMD programs, sanctions should be applied to the procurement of materials and technology stage. Targeted financial sanctions on individuals and entities involved in these networks will disrupt their ability to transfer funds and will help to starve the programs of necessary goods and materials and slow technical development. They will also influence global private sector business, which may be inclined to cut off business relationships with anything remotely

linked to the sanctioned entity unless clear guidance for what is more narrowly prohibited is set out.

Targeting program fundraising activities is the best way to disrupt mature programs that are largely self-sufficient and rely only to a small extent on overseas procurement. This may be difficult, since it might be necessary for sanctions implementers to target a state's entire economy to ensure that states cannot divert revenue to weapons of mass destruction programs. Sanctions or other controls should focus on individuals or entities managing the programs and also on sectors of the economy that generate revenue for the programs (sectoral sanctions) or on revenue-generating exports.

Targeting program fundraising activities is the best way to disrupt mature programs that are largely self-sufficient and rely only to a small extent on overseas procurement.

Better Financing of Proliferation Safeguards

The current failure of the international community to counter the threat from North Korea's nuclear and other WMD programs, and past failures to deal with India's and Pakistan's nuclear programs, shows clearly the need to strengthen defenses against proliferating states. This includes measures to combat proliferation finance. The areas where action is needed are listed below. The CNAS project on identifying and countering proliferation finance is preparing detailed recommendations for specific actions in these areas. These will be published in 2018 and will cover the following basic recommendations:

Strengthen International Control Regimes

BUILD ON THE BASIC COMPONENT OF THE INTERNATIONAL FRAMEWORK TO CONTROL FINANCING OF PROLIFERATION, U.N. SECURITY COUNCIL RESOLUTION 1540 (2004)

Because it does not carry some of the negative political connotations of Security Council sanctions regimes, many U.N. member states can more easily embrace provisions of Resolution 1540 (2004). U.N. Security Council Resolution 2325 (2016) directs the 1540 Committee to intensify efforts to promote implementation of Resolution 1540 (2004) including provisions relating to countering proliferation finance.[40] The United Nations should strengthen generic controls. Member states must support the 1540 Committee and provide technical assistance to those states which have genuine difficulties implementing measures on FoP because they lack expertise, resources, or guidance.

LOOKING BEYOND U.N. SECURITY COUNCIL RESOLUTIONS REGARDING NORTH KOREA AND IRAN

It is almost certainly too late to halt North Korea's nuclear program, or even to slow it appreciably. However, the small numbers of implementation reports submitted by member states, and their limited content, clearly demonstrate that the overall level of implementation by U.N. member states is low. Gaps in what is supposed to be a fully implemented sanctions regime encourage North Korea to believe that no U.N. consensus against its programs exists, and that likely weaknesses in the sanctions framework could be exploited.

The U.N. should strengthen its conceptual framework of financial sanctions. Guidelines for comprehensive implementation need to be on the shelf in case a new proliferating state emerges in the future, or Iran takes advantage of termination of the majority of JCPOA restrictions in 2015 to renew nuclear and other WMD-related activities.

MORE WORK ON FOP BY THE FINANCIAL ACTION TASK FORCE

Current FATF standards to counter the FoP threat are insufficient. FATF should extend its standards to cover the range of U.N. financial sanctions on WMD programs. To date, many FATF recommendations relevant to FoP are couched only in terms of money laundering and terrorist financing. FATF must make those recommendations equally applicable to financing of proliferation.

INFORMATION SHARING WITHIN THE EGMONT GROUP

Members of the Egmont Group, an informal network of financial intelligence units (national centers that collect and process information supplied by the financial sector and other entities on suspicious financial activity) should work to make their activities a reliable channel for circulating generic information on financing of proliferation threats. To date, most information shared within the Egmont Group relates to specific casework, but education on broader typologies would be important for assisting states to conduct FoP risk assessments.

FACTORING FINANCING OF PROLIFERATION IN MULTILATERAL EXPORT CONTROL REGIMES

Multilateral export control regimes should assess the potential value of controls on financing of proliferation to their objectives, and provide guidance accordingly to their members.

Strengthening Controls at The National Level

BOLSTERING NATIONAL REGIMES

The FATF Asia/Pacific Group, the United Nations Office of Drugs and Crime (UNODC), the United Nations Regional Centre for Peace, Disarmament, and Development in Latin America and the Caribbean (UNLIREC), the U.S. Department of State and the Defense Threat Reduction Agency, and the EU have organized outreach and training workshops on the financing of proliferation threat. Further capacity-building efforts should focus on financing of proliferation risk assessments, legislation, domestic coordination and communication, and information sharing with international partners.

Government and private sector actors should collaborate on enhancing communications on proliferation finance threats. Counter-proliferation actions are most likely to be successful when regarded as a joint endeavor between government and the private sector.

Conclusions

Financing of proliferation of WMD should be understood both as a serious threat to the international financial system and as a potentially key tool to combat proliferation. Policymakers will see the growing importance of countering proliferation finance from a variety of sources. North Korea's continuing nuclear and missile tests underscore the immediate security implications of its sophisticated proliferation networks. FATF's current work to revise its guidance serves as a focus for multilateral action. Civil society actively complements these efforts: Outreach activities of proliferation finance-related projects funded by official sources (such as the Project Alpha study) and non-official sources (such as the current study) and discussions of FoP at private sector meetings all draw attention to the need to focus on FoP and strategies to impede this illicit financial activity.[41]

The international community must strengthen the global framework of financial controls; otherwise, proliferation networks will continue to deliver illicit capability to states such as North Korea. In the short term the emphasis should be on better implementation of existing controls, which necessarily must be the basis of future actions. The U.N. Security Council, FATF, the Egmont Group, multilateral export control regimes, national authorities, and FIs all have work to do to advance this crucial goal.

It is almost certainly too late for financial sanctions or other FoP controls to prevent North Korea achieving nuclear weapons capability, however the current restrictions on Iran's nuclear program will largely fall away in 2025, and putting in place now a strengthened framework to identify and disrupt FoP will enhance the international community's options to monitor and if necessary restrain the program after 2025. Identification and disruption of FoP also could play a key role in identifying and constraining any future nuclear or other WMD programs initiated by states in Asia, the Middle East, or elsewhere.

The United States is uniquely well placed to lead the way in this crucial work. The nation has spent decades prioritizing disarmament and nonproliferation as a priority for the international community. It has taken the lead on facing proliferation threats from North Korea and Iran, both on its own initiative as well as within multilateral coalitions and at the U.N. Security Council. The U.S. financial sector has a mature culture of regulatory compliance with regard to money laundering and terror financing, and American law enforcement and

intelligence agencies are closely focused on mapping networks of proliferation. Given this experience, the United States should take an active role in the United Nations, FATF and the other international bodies whose activities are potentially impacted by FoP.

A strengthened FoP framework will enhance options to monitor and if necessary restrain Iran's nuclear program after 2025.

Endnotes

1. Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation, Final Report," (Project Alpha, King's College London, October 13, 2017), https://projectalpha.eu/final-report-typologies-of-proliferation-finance/.

2. See, for example, *Appendix F: Money Laundering and Terrorist Financing "Red Flags"* of the Bank Secrecy Act Anti-Money Laundering Examination Manual, particularly the red flags for trade finance, Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, Appendix F: Money Laundering and Terrorist Financing "Red Flags," Trade Finance, https://www.ffiec.gov/bsa_aml_infobase/pages_ manual/olm_106.htm; and "The Wolfsberg Group, ICC and BAFT Trade Finance Principles," http://www.wolfsberg-principles.com/pdf/home/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.

3. The export control lists include those of the Nuclear Suppliers Group and the Missile Technology Control Regime. United Nations Panel of Experts, "Final report of the Panel Experts established pursuant to resolution 1929 (2010)," S/2014/394 (United Nations Security Council, June 2014), https://www.un.org/ga/search/view_doc.asp?symbol=S/2014/394.UN.

4. "Treasury Takes Action to Further Restrict North Korea's Access to the U.S. Financial System," United States Department of the Treasury, press release, June 1, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0471.aspx.

5. In some jurisdictions, the United States, for example, financial transactions connected with a property involved in unlawful activity are categorized as money laundering. Statistics relating to cases of financing of unlawful exports of proliferation – related items, for example, would be recorded as money laundering rather than financing of proliferation, which may be an additional factor to be considered when conducting FoP risk assessments.

6. Juan Manuel Vega-Serrano, "FATF President Juan Manuel Vega-Serrano's remarks at the meeting of the U.N. Security Council, December 15, 2016," http://www.fatf-gafi.org/fr/publications/financementdelaproliferation/documents/speech-vega-serrano-un-security-council-meeting-dec2016.html?hf=10&b=0&s=desc(fatf_releasedate).

7. Ellen Nakashima, Anna Fifield, and Joby Warrick, "North Korea could cross ICBM threshold next year, U.S. officials warn in new assessment," *The Washington Post*, July 25, 2017, https://www.washingtonpost.com/world/national-security/north-korea-could-cross-icbm-threshold-next-year-us-officials-warn-in-new-assessment/2017/07/25/4107dc4a-70af-11e7-8f39-eeb7d3a2d304_story.html?utm_term=.78c39137fff7.

8. See endnote 12.

9. Brewer, "Study of Typologies of Financing of WMD Proliferation." In the course of cyber attacks on February 4, 2016, targeting the Bangladesh Central Bank, $81 million U.S. was diverted to casinos in the Philippines. The group responsible, Lazarus, may be based in North Korea, and most of the funds are still missing. It would appear possible that at least some may have been diverted to finance North Korea's WMD program. The funds sit outside North Korea and could have been placed relatively easily into the international financial system for this purpose.

10. A "ledger" system refers to an accounting arrangement in which linked companies maintain a record of transactions made on each other's' behalf. Over a period of time, the companies may need only infrequently to transfer funds between institutions or firms to settle accounts.

11. See cases 3 and 5 (relating to North Korea) and 17 (Iran) in Brewer, "Study of Typologies of Financing of WMD Proliferation."

12. See, inter alia, United States Department of the Treasury Financial Crimes Enforcement Network, *Advisory on North Korea's Use of the International Financial System: North Korea uses front and trade companies to disguise, move, and launder funds to finance its nuclear and ballistic missile programs*, FIN-2017-A008, November 2, 2017, https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Financing%20Advisory%20FINAL%2011022017_0.pdf2017.

13. Financial Action Task Force, "Typologies Report on Proliferation Financing," FATF, June 18, 2008, http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html.

14. See various United Nations Panel of Experts Reports: On Iran: "Final report of the Panel of Experts established pursuant to resolution 1929 (2010)," 2014, United Nations Security Council document S/2014/394, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2014/394); "Final report of the Panel of Experts established pursuant to resolution 1929 (2010)," 2015, United Nations Security Council document S/2015/401, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/401). On DPRK: "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," 2016, United Nations Security Council document S/2016/157, http://www.un.org/ga/search/view_doc.asp?symbol=S/2016/157; "Report of the Panel of Experts established pursuant to resolution 1874," 2017, United Nations Security Council document S/2017/150, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150.

15. United States Department of Justice, *Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases: January 2014 to the present: updated February 17, 2017*, https://www.

pmddtc.state.gov/compliance/documents/ Ongoing-ExportCaseFactSheet.pdf.

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

17. Prior to 1998, no sanctions were applied to India's nuclear program (although some countries applied export controls) and only limited US sanctions were applied to Pakistan's nuclear program. Following the nuclear tests in 1998 by Pakistan and India the U.S. and other countries imposed sanctions on both. U.S. sanctions were lifted in September 2001.

18. See Case 11 of Brewer, "Study of Typologies of Financing of WMD Proliferation"; Wikileaks, "Australia Group 2008 Information Exchange," http://www.telegraph.co.uk/news/wikileaks-files/nuclear-wikileaks/8297102/AUSTRALIA-GROUP-2008-INFORMATION-EXCHANGE-IE.html.

19. Committee on the Global Financial System, "Trade Finance: Developments and Issues," Paper No 50, (Bank for International Settlements, January 2014); conversely figure 41 of the ICC Banking Commission's paper "2017 Rethinking Trade & Finance" suggests a decrease in use of letters of credit since 2009 of only about 10. percent. International Chamber of Commerce, "Rethinking Trade & Finance," (ICC Banking Commission, March 2017), https://cdn.iccwbo.org/content/uploads/sites/3/2017/06/2017-rethinking-trade-finance.pdf.

20. "The Wolfsberg Group, ICC and BAFT, Trade Finance Principles."

21. However, even where trade financing documentation is available, many financial institutions may conduct checks focused primarily on credit risk. Dubai Financial Services Authority Trade Finance Report 2016, http://www.dfsa.ae/Documents/ThematicReviews/TF-Report-FINAL%20Eng%2012%20october%20 2016%20mid-res.pdf.

22. Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "Terrorist use of Virtual Currencies Containing the Potential Threat," (CNAS, May 2017).

23. Martin Arnold, "European banks to launch blockchain trade finance platform," *Financial Times*, June 26, 2017, https://www.ft.com/content/6bb4f678-5a8c-11e7-b553-e2df1b0c3220.

24. FAQ No 10 from 1540 Committee, "Frequently Asked Questions on Resolution 1540 (2004)," U.N. 1540 Committee website, http://www.un.org/en/sc/1540/faq.shtml#10.

25. United Nations Security Council, "Report of the Security Council Committee established pursuant to resolution 1540 (2004)" (United Nations Security Council, 2016), S/2016/1038, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/1038.

26. Kenneth L. Bachman and Paul Marquardt, "Understanding U.S. Sanctions," Cleary Gottlieb, May 15, 2012, http://c.ymcdn.com/sites/www.iib.org/resource/resmgr/imported/2012.AML.Bachman.pdf.

27. Ibid.

28. See Paragraph 12 in United Nations Panel of Experts, "Final report of the Panel Experts established pursuant to resolution 1929 (2010)," S/2014/394 (U.N. Security Council, June 2014), https://www.un.org/ga/search/view_doc.asp?symbol=S/2014/394.UN.

29. Reports submitted to date are listed at: https://www.un.org/sc/suborg/en/sanctions/1718/implementation-reports.

30. RUSI APG Implementation Guide and Model Law for Governments, posted October 17, 2017, http://www.apgml.org/documents/.

31. FATF, "Consolidated Assessment Ratings" (FATF, December 15, 2017), http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf.

32. See Paragraph 8(d) in United Nations Security Council resolution 1718 (2006), *Imposition of an arms embargo, assets freeze and travel ban on persons involved in the DPRK's nuclear programme, and a ban on a range of imports and exports, to prohibit the DPRK from conducting nuclear tests or launching ballistic missiles*, S/RES/1718 (October 14, 2006), http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1718%20%282006%29, 3.

33. See "Interpretive Note to Recommendation 7: Targeted Financial Sanctions Related to Proliferation" in FATF, "The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" (FATF, February 2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

34. The cases involved violations of the International Emergency Economic Powers Act (IEEPA) and related money-laundering legislation.

35. See, for example, United Nations, Panel of Experts established pursuant to resolution 1874 (2009), *Midterm report of the Panel of Experts established pursuant to resolution 1874 (2009)*, S/2017/742 (September 5, 2017), http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/742, 39; and United Nations, Panel of Experts established pursuant to resolution 1929 (2010), *Final report of the Panel of Experts established pursuant to resolution 1929 (2010)*, S/2015/401 (June 2, 2015), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2015_401.pdf, 29.

36. As set out in Recommendation 2 of the FATF Standards of 2012 FATF Recommendation 2 sets the specific standard for interagency coordination. See FATF, "The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" (FATF, February 2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

37. As set out in Recommendation 40 of the FATF Standards of 2012. FATF, "The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," (FATF, February 2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

38. In some jurisdictions, the United States for example, financial transactions connected with a property involved in unlawful activity are categorized as money laundering. Statistics relating to cases of financing of unlawful exports of proliferation-related items, for example, would be recorded as money laundering rather than FoP, which may be an additional factor to be considered when conducting FoP risk assessments.

39. See also discussion in Emil Dall, Tom Keatinge, and Andrea Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions," Guidance Paper (Royal United Service Institute, April 2017), https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf.

40. United Nations Security Council resolution 2325 (2016), On non-proliferation of nuclear, chemical and biological weapons, S/RES/2325 (December 15, 2016), https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2325(2016).

41. For example, panel discussion on the subject "A Clear and Present Danger: Developing Models to Combat Proliferation Financing" (ACAMS 16th Annual AML and Financial Crime Conference, Las Vegas, September 25, 2017), https://acams.digitellinc.com/acams/sessions/494/view.

42. Table modified from Table 2 of Brewer, "Study of Typologies of Financing of WMD Proliferation," 20.

43. The financial operations of Chinpo Shipping (Private) Ltd. are described in the 2016 Final Report of the DPRK Panel of Experts.

About the Center for a New American Security

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

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

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

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

Bold. Innovative. Bipartisan.