CNAS

NOVEMBER 2018

The Financing of WMD Proliferation

Conducting Risk Assessments

By Dr. Jonathan Brewer

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 the financing of proliferation. 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 UK 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 (2003–2004). He was Head of Counter-Proliferation 2005–2010.

Acknowledgements

The author would like to thank Adam Klein and Loren DeJonge Schulman 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. Early versions of this paper benefited greatly from comments made in their personal capacities by a number of banking experts, including Graham Finding, Graham Baldock, Eda Erol, Albrecht Küstermann, and others.

Cover Photo: CNAS Illustration/Melody Cook

THE FINANCING OF WMD PROLIFERATION

Conducting Risk Assessments

Executive Summary

KEY TAKEAWAYS

- Despite the threat from the financing of proliferation of nuclear and other weapons of mass destruction (WMD), only a handful of governments and companies are taking meaningful steps to counter it.
- This paper outlines the various sources of the threat, the international control framework, and how authorities and financial sector actors fit into the countering proliferation finance regime. Effective partnership between them is essential to identifying and countering the threat.
- The paper describes how authorities and financial institutions should conduct proliferation financing risk assessments, a necessary first step to take to protect themselves, and the indicators to take into account and procedures to follow.

The proliferation of weapons of mass destruction is a critical threat facing the international community. Numerous United Nations Security Council Resolutions (UNSCRs) place binding obligations on member states to put in place measures to combat proliferation threats, whether from non-state actors, including terrorist groups, or specific state actors like North Korea. Among the tools to counter the spread of WMDs is the adoption of policies designed to deter, disrupt, and eliminate the financing of proliferation.

In recent years, international organizations, with significant input from concerned parties like the United States, have offered guidance to financial institutions on countering proliferation finance (CPF). In particular, the Financial Action Task Force (FATF), the international financial crimes standard-setter, has tried to address the fact that not all national governments or banks understand what proliferation finance is, how to identify it, and how to put in place measures to combat it. But proliferation finance is difficult to detect, and even among the most effectively governed jurisdictions, whose financial institutions are among the largest, most well-resourced, and most focused on combating financial crimes, it is very difficult to track proliferation financing activity.

Fortunately for national governments and financial institutions, there are no insuperable obstacles to building a stronger regime to counter proliferation finance. Among the first steps in understanding and combating proliferation finance is understanding the risk exposure of individual jurisdictions and their financial institutions. This paper offers guidance to national authorities and to financial sector actors on the components of such a risk assessment, including sources of proliferation risks, indicators, and how financial institutions should monitor customers' profiles and behavior to detect proliferation financing.

Importantly, this paper offers a points-based blueprint for measuring specific levels of proliferation finance risk, which financial institutions could use as benchmarks against which to monitor their customers and their businesses.

Conducting a proliferation financing risk assessment is a necessary first step to enable authorities and financial institutions to understand the threat and identify measures necessary for mitigation. Proliferation financing risk assessments do not require authorities or financial institutions to put in place new business procedures. They can be conducted by adapting existing procedures for assessing risks of money laundering or terrorist financing. This paper shows how this can be done.

Fortunately for national governments and financial institutions, there are no insuperable obstacles to building a stronger regime to counter proliferation finance.

Introduction

The proliferation of nuclear and other weapons of mass destruction (WMD) is a fundamental threat to global security; every United Nations member state has an obligation to prevent WMD proliferation. Disrupting financing is a potentially valuable tool to counter proliferation. Alarmingly, and to the benefit of proliferators and rogue regimes, only a handful of governments and companies are aware of and meaningfully engaged in this work.

There is no insurmountable barrier to conducting a much stronger global campaign to combat proliferation financing. Even moderate enhancements could limit the most dangerous proliferators and increase global security. But such enhancements require both governments and banks to go beyond simply complying with the letter of the law regarding targeted financial sanctions, money laundering, and terrorist financing.

Governments and financial institutions face many challenges in curbing the financing of proliferation. Few governments or banks understand what financing of WMD proliferation looks like. Moreover, few have attempted to assess their vulnerability to the threat. For example, many do not know how financial institutions without direct links to North Korea or other proliferating states might be exposed through activities of correspondent banks. They may also not know how exposed they are when conducting business in neighboring areas such as China and East Asia. Understanding and combating proliferation-finance threats requires not only local knowledge and local efforts, but also global and multilateral coordination.

This paper builds on recent work by the U.N. and independent scholars on such threats.[1] It considers the steps that governments and banks could take to conduct risk assessments of the financing of WMD proliferation:

- Understanding the threat,
- Assessing the context-specific risk, and
- Implementing a plan to mitigate this risk.

These steps, taken collectively, will help governments and the financial sector to promote global security and protect the integrity of our financial system.

Ultimately, combating proliferation is a joint endeavor. The work is a public-private partnership, played out at the international, national, and private-sector levels. The effort requires coordination among national financial authorities, intelligence and security agencies, and international banks and companies. By itself, disrupting the financing of proliferation is unlikely to halt WMD programs that are already far advanced. However, it can slow further WMD development or maintenance, and provide space for policymakers to negotiate solutions to promote international peace and security.

Lay of the Land

What Constitutes Financing of WMD Proliferation?

There are no U.N. resolutions focused specifically on financing of proliferation. Furthermore, there is neither a U.N. definition of financing of proliferation nor a financing-of-proliferation equivalent of the U.N. Terrorist Financing Convention. However, as argued in the Center for a New American Security's primer on financing of proliferation,[2] there is an acceptable alternative to a U.N. standard: the 2010 working definition developed by the Financial Action Task Force (FATF),[3] the global-standard-setting body on money laundering and terrorist financing:

> '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

Under this definition, a large range of industrial and commercial activities could potentially be at risk from proliferation financing, so a variety of different types of financial institutions could be caught up, depending on the scope of their business.[4] Furthermore, jurisdictions potentially affected could be far removed from proliferating states. Second, most WMD proliferation in recent years does not involve the purchase or transport of finished weapons systems (although this should not be ruled out). Instead, most proliferation involves overseas procurement of basic materials and equipment needed to construct WMD. Third, financing-of-proliferation legal liability can arise both from U.N. Security Council measures (e.g., those concerning North Korea and Iran) and from national legislation, such as export controls imposed by countries on materials or equipment intended for Pakistan's or India's WMD program.

What Are the Sources of Financing-of-Proliferation Threats?

The proliferation threat arises from the activities of a small number of countries that have developed, or are suspected of developing, illicit nuclear, biological, or chemical weapons systems. These states will generally declare that they need these weapons for defensive purposes. However, neighbors may interpret these programs as threatening and decide to develop similar weapons in response. This reaction undermines international nonproliferation regimes, with potentially profound implications for international peace and security. The main countries to consider as actual or potential risks in the context of nuclear proliferation are set out in the table below.[5]

WMD programs involve activities ranging from the construction and maintenance of infrastructure and equipment within the proliferating state to the procurement of items such as materials or machinery from overseas suppliers. All of these need to be paid for. Some inputs, such as highly enriched uranium or biological toxins, are dangerous and carefully protected. Other items are dual-use; these include high-grade aluminum alloy and corrosion-resistant valves. However, the majority of required materials are standard industrial items, with many uses. Most proliferators prefer to source items from high-grade manufacturers in the United States or Europe. When they cannot do so, they look for manufacturers elsewhere—for example, in India or China.[7]

Ultimately, combating proliferation is a joint endeavor. The work is a public-private partnership, played out at the international, national, and private-sector levels.

The Geography of Financing of Proliferation Risks

Non-NPT States That are Expected to Maintain or Improve Nuclear Capabilities Via Illicit Overseas Procurement	Potential Nuclear Weapon States Dependent on Illicit Overseas Procurement	States That Might Consider Developing a Nuclear Weapons Capability Via Illicit Overseas Procurement (Perhaps Due to North Korea's WMD Program)	States That Might Consider Developing a Nuclear Weapons Capability Via Illicit Overseas Procurement (Perhaps Due to Developments in Iran)
Pakistan	Iran	South Korea *(Low Probability)*	Egypt *(Low to Medium Probability)*
India		Taiwan *(Low)*	Algeria *(Low)*
North Korea		Japan *(Low)*	Turkey *(Medium)*
Israel (on occasion)			Saudi Arabia *(Medium)*
			Syria *(Low, Given Civil War)*
			Failed States in Africa and Asia *(Low)*

This chart shows the main countries to consider when assessing proliferation-financing risk in the next five to ten years. It is adapted from work carried out by Albright and others. The countries named either purchase equipment and materials for nuclear weapons programs from overseas illicitly or would need to.[6] China might fall into this category, but is excluded from the table because of its status as an NPT (Treaty on Non-Proliferation of Nuclear Weapons) nuclear weapon state. Other developed countries, not listed, might also need to depend on illicit overseas procurement if they decided to build a nuclear weapons program in the future.

Proliferation-Financing Obligations and Their Implementation

WMD proliferation is controlled globally by a framework of U.N. Security Council resolutions. Resolution 1540 (2004) and successor resolutions impose obligations on member states to prevent proliferation of WMD and related materials to non-state actors.[8] These include generalized requirements to prevent financing that would contribute to proliferation. In addition, country-specific U.N. resolutions (on North Korea and Iran) require states to implement a range of financial measures to address aspects of financing of proliferation, including targeted financial sanctions, activity-based sanctions, sectoral sanctions, vigilance, and other financial requirements.[9] FATF has published guidance on the implementation of these U.N. resolutions.[10] U.N. member states are expected to incorporate these requirements into their domestic legislation. In practice, they do so with varying effectiveness.

Some states also place controls on exports to specific WMD programs (e.g., those of Pakistan or India) or on dual-use goods or materials that could be used in WMD programs in general. These controls may extend to finance or financial services. However, although most states have laws regarding U.N. financial measures, domestic export controls, and related financial crime, very few countries legislate specifically against financing of proliferation.[11] As will be explained below, the scarcity of national-level legislation imperils the global fight against WMD proliferation and exposes inattentive countries' financial sectors to regulatory and reputational risks.

Financial institutions typically adopt a mix of rules-based and risk-based procedures to comply with legislation on financial crime and sanctions. Rules-based systems ensure that an institution's business is compliant with targeted financial sanctions by screening transactions against lists of individuals and entities designated by the U.N., EU, United States, and other countries. Risk-based transaction-monitoring systems, calibrated to match an individual institution's risk appetite and usually purchased from commercial vendors, are designed to identify money laundering and other financial crimes, not financing of proliferation.

However, financial institutions should be proactive in developing their defenses against financing of proliferation, and these measures alone are insufficient. Few banks, for example, currently incorporate financing-of-proliferation risks into their risk assessments. Furthermore, WMD financiers are adept at circumventing targeted sanctions by operating through front companies and complex financial networks. They exploit jurisdictions whose financial or export-control systems are perceived as weak or easy to circumvent, or jurisdictions with political, trade, commercial/financial, or historic links to countries with WMD programs.[12]

Because of these circumvention schemes, governments or financial institutions without direct links to North Korea or other proliferating states can still be exposed to their programs or networks. The factors that result in exposure include activities of correspondent banks and trading companies, and business conducted in neighboring regions (e.g., China and East Asia) or other areas where proliferation networks may be active. As recently noted by the under secretary for terrorism and financial intelligence at the U.S. Treasury, financial institutions' compliance programs need to be proactive given the sophisticated ways actors move money and goods.[13]

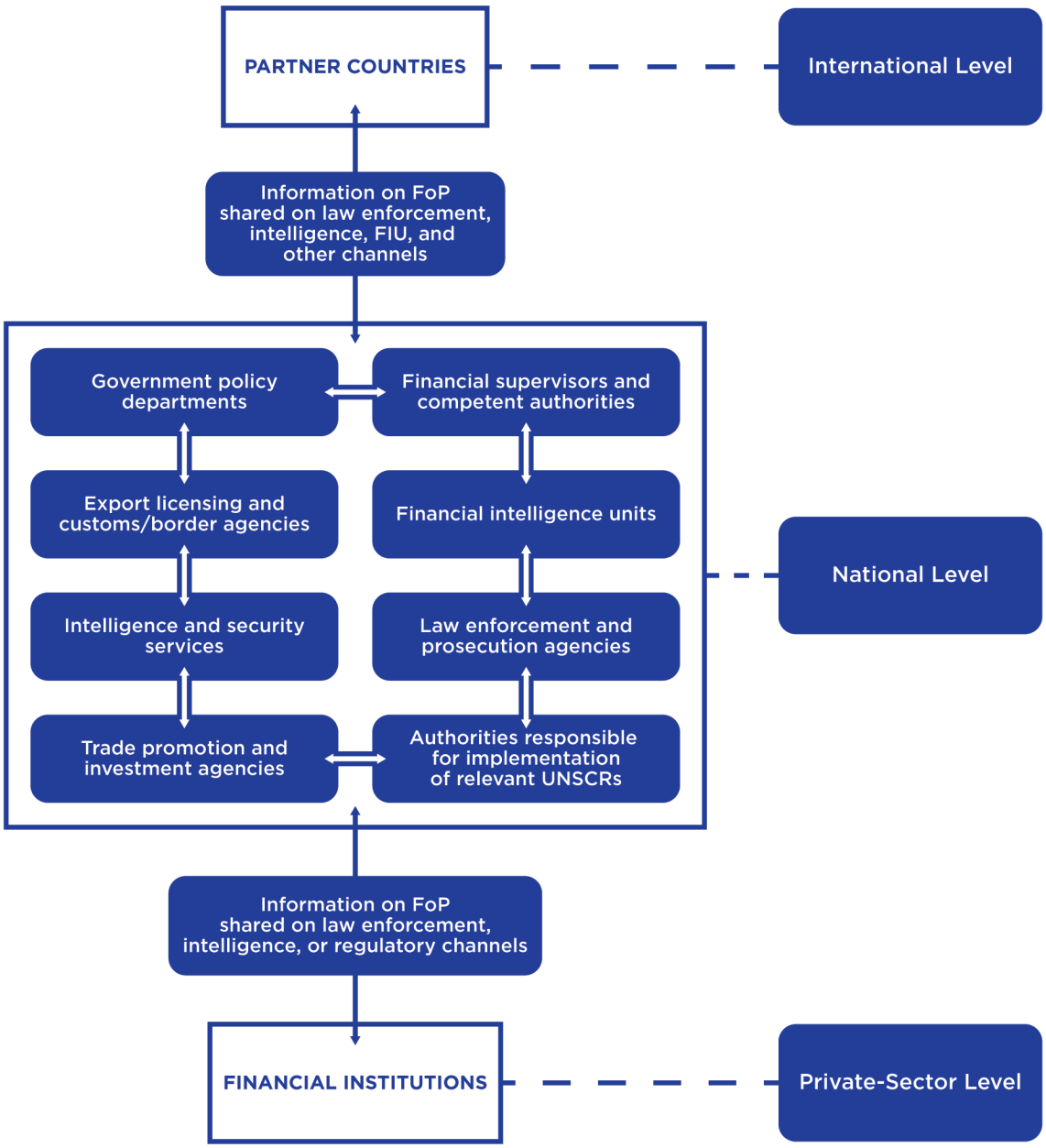
> **Financial institutions should be proactive in developing their defenses against financing of proliferation.**

Many financial institutions question the extent to which they, in isolation, should be playing a role in countering WMD proliferation. They argue that exporters or traders should be the front line of controls, because they are the ones who need licenses for exports of dual-use or other strategically sensitive goods and so should have a better understanding of proliferation-sensitive equipment and materials.

Financial transactions connected with proliferation-sensitive materials and equipment are difficult to differentiate by themselves from financial transactions connected with legitimate trade. Furthermore, unless financial institutions are involved in trade financing, they will probably not have access to sufficient information to distinguish whether proliferation-sensitive materials and equipment are involved.[14] Presently only a minority (perhaps 20 percent) of international trade involves trade finance. The remainder is conducted on "open account" terms[15] and settled by wire transfers that carry little or no information about the nature of the transaction, such as goods, shipping routes, and the like.[16]

In addition, although proliferation networks can reach across the globe, financial institutions may process transactions from only a small part and so do not have sufficient information to enable identification of the complete network. Under these circumstances, financial institutions argue, simple transaction-level controls are not effective at identifying financing of proliferation, or

Figure 1: Levels of Cooperation on Combating Proliferation Finance

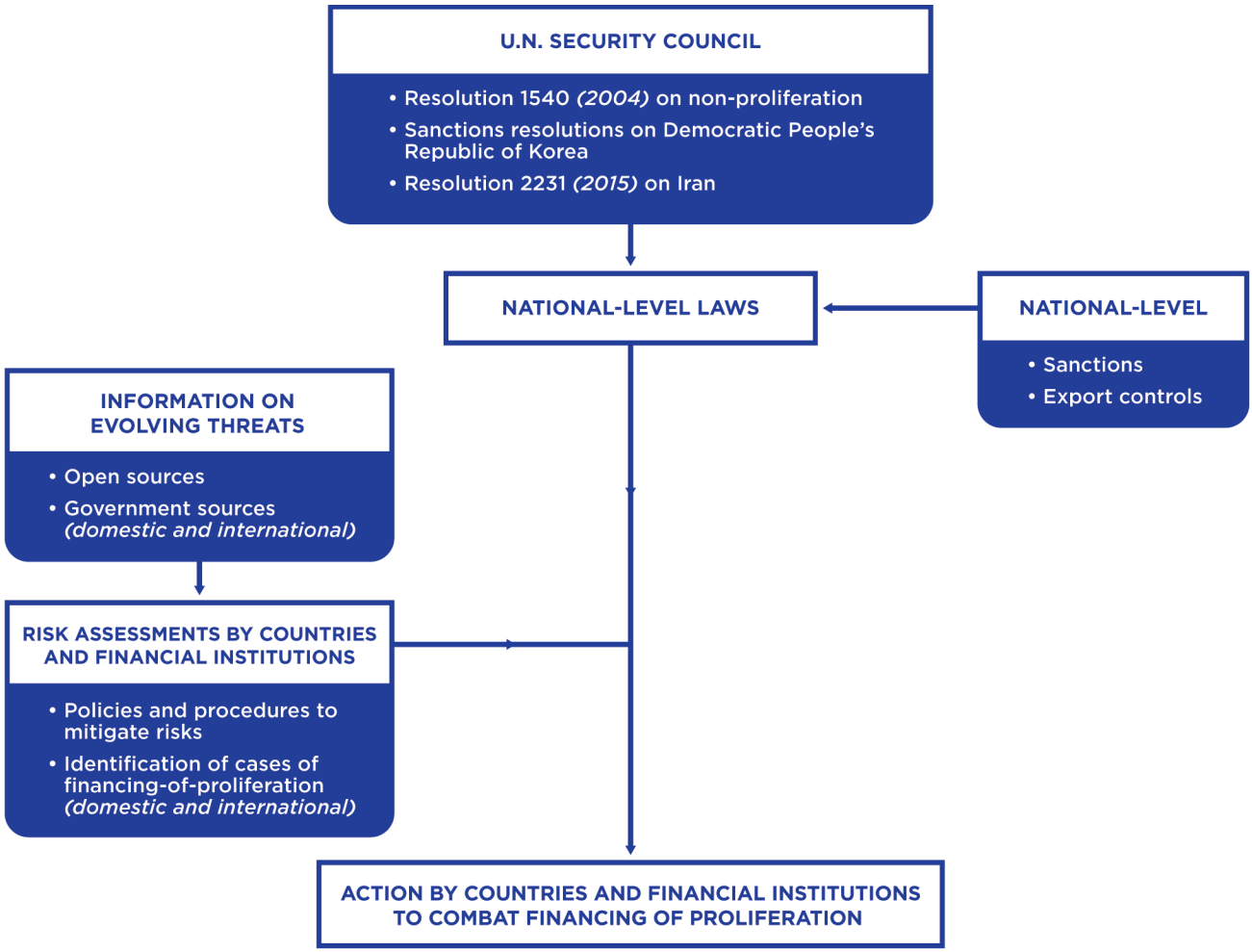


indeed other financial crime.[17]

However, many financial institutions also argue that even though they do not have the ability to screen transactions for financing of proliferation in real time, nor identify financing of proliferation through analysis of their financial databases, their databases can be useful for analysis and investigation when combined with open-source information or intelligence shared by governments.[18] In fact, combating WMD-proliferation networks, because of their geographical spread and complexity, requires information sharing at many levels. Governments need to share sensitive intelligence about proliferation with international partners, and they also need to share such information among the potentially wide range of domestic departments and agencies that have a role in combating proliferation and its financing. Figure 1 illustrates how the different elements ideally fit together.

Because the proliferation-financing threat varies across different regions and industries, building

Figure 2: Components of an Effective Response to the Financing of Proliferation



cooperative relationships should be a key objective of both host governments and financial institutions. Governments need to declassify intelligence for use by financial institutions. Financial institutions should also be monitoring open-source information for geopolitical developments.

Combating financing of proliferation is a collaborative endeavor. Success is unlikely without close communication and coordination between the organizations shown here at international, national, and private-sector levels. Having put in place information-sharing arrangements, governments and financial institutions must then develop effective policies, and procedures and enhance their analytical capabilities to address financing-of-proliferation risk. Figure 2 illustrates how these points fit together.

Table 1: Some Sources of Information on Financing of Proliferation[22]

Publication	Description
FATF 2008 Typologies Report	Describes financing-of-proliferation case studies and indicators.
Jersey Financial Services Commission Report *(2011)*	Describes financing-of-proliferation indicators.
Royal United Services Institute Reports	Offer guidance for governments and financial institutions on combating financing of proliferation.
C4ADS Reports	Describe characteristics of North Korean financial networks.
King's College London Project Alpha Typologies Report *(October 2017)*	Describes financing-of-proliferation case studies (including nuclear, biological, and chemical examples) and indicators.
CNAS' "The Financing Of Nuclear And Other Weapons Of Mass Destruction Proliferation" *(January 2018)*	A financing-of-proliferation primer.
U.S. Department Of The Treasury Financial Crime Enforcement Network Advisory On North Korea's Use Of International Financial System *(November 2017)*	Describes red flags of potential North Korean illicit financial activity.
Latvian Financial And Capital Market Commission Press Release *(July 2017)*	Records that customers of JSC "NORVIK BANKA" and JSC "Rietumu Banka" used offshore companies and complicated chain transactions to circumvent international sanctions on North Korea. Notes that similar activities took place at three other Latvian banks.
U.S. Department Of Justice Annual Summary Of Major U.S. Export Enforcement, Economic Espionage, Trade Secret And Embargo-related Criminal Cases *(January 2015 to the present: updated January 19, 2018)*	Briefly describes some major export enforcement, economic espionage, theft-of-trade-secrets, and embargo-related criminal prosecutions. Updated annually. About 10-15% of the cases in the 2017 report included information relevant to financing of proliferation.
FATF Guidance On The Implementation Of Financial Provisions Of U.N. Security Council Resolutions To Counter WMD Proliferation *(March 2018)*	Guidance covering implementation of the range of U.N. financial sanctions on WMD programs, including references to typologies and risks.

Basic Principles for Conducting Financing-of-Proliferation Risk Assessments

Although the nature of financing-of-proliferation threats is different, the principles underlying a strategy to counter them are similar to those underlying strategies to counter money-laundering and terrorist-financing threats. The process of developing this strategy must begin with an assessment of proliferation-financing risk. Risk assessments provide governments and financial institutions with a clear picture of the sources of WMD-proliferation-financing threats. They also clarify the likelihood of impact on national security or the financial services sector. A risk assessment builds on a process that most countries and financial institutions are already familiar with. FATF's 2012 Standards require countries to carry out national risk assessments to address threats from money laundering and terrorist financing.[19] FATF also mandates that countries require financial institutions "to identify, assess and understand their [money-laundering] and [terrorist-financing] risks" and to "manage and mitigate" these risks.[20]

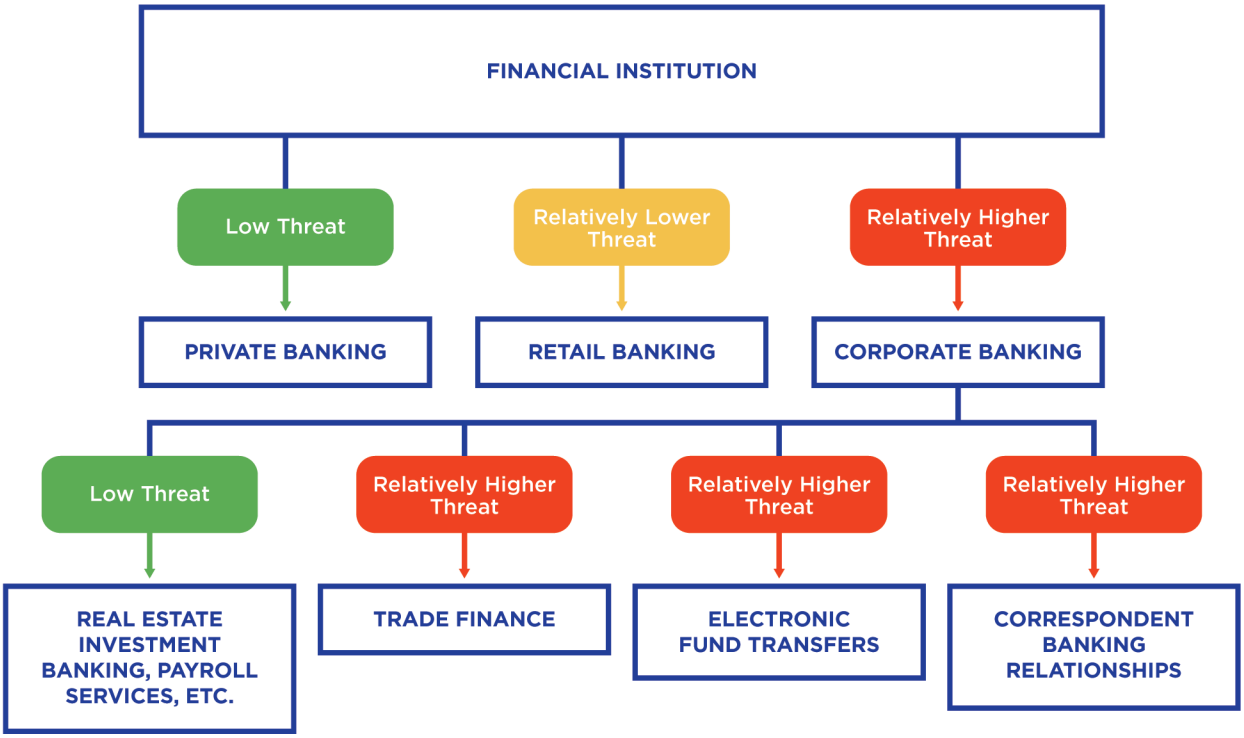
FATF does not currently require countries to include proliferation-financing risk in its national risk assessments. It should do so. Until then, government and banks need to adapt existing guidance from money-laundering and terrorist-financing risk assessments.[21]

Sources of Financing-of-Proliferation Threats

Understanding the range of possible financing-of-proliferation threats is the first step in evaluating financing-of-proliferation risk. Table 1 outlines a selection of authoritative, recent sources of information on characteristics and typologies of financing of proliferation. The list is not exhaustive. Other official and unofficial sources should also be monitored.

The risk assessment procedures discussed in this paper are derived from cases of financing of proliferation described in the King's College London Project Alpha Report. That report identifies indicators of possible financing of proliferation that are summarized in Annex 1. The scope and detail of individual indicators vary, reflecting the variety of cases in the report.

Figure 3: The Threat Profile of Different Banking Activities



Schematic representation of relative levels of financing-of-proliferation threats to different areas of banking activity, products, and services. The banking categories are indicative and not exhaustive.

Table 2: Institution-specific Financing of WMD Proliferation Risk

Type of Institution	Activities Carried Out by These Institutions That Entail Possibly Higher Risk of WMD-Proliferation Financing
Insurance Business	Insuring international trade and trade credit, or transport and shipping
Money Service Business	Money remitting and transferring
Designated Nonfinancial Businesses and Persons and Other Institutions, e.g. • Lawyers • Gold Trader • Cash Couriers • Trust and Company Service Providers (including company formation agents)	 • Legal services • Gold trading • Cash transportation • Trust and company service managements (including company formation services)

This table is adapted from Table 1 in FATF's "National Money Laundering and Terrorist Financing Risk Assessment" of February 2013. It is not intended to be a comprehensive listing of types of financial institutions potentially at risk from financing of WMD proliferation.[25]

Financial System Vulnerabilities

Countries' and financial institutions' vulnerability to financing of WMD proliferation depends on a number of factors. These include whether there exist relationships with institutions or jurisdictions where proliferators operate, the extent of general trade business, and whether financial institutions' customers or counterparties deal with WMD technologies or components.[23] FATF has listed some general principles for identifying high-risk customers and transactions.[24] The nature of the financial services offered by individual financial institutions is also important (Figure 3). Corporate banking activities (or other banking activities exposed to international trade) are most exposed to the financing-of-proliferation threat, because overseas procurement by WMD programs exploits international trade mechanisms. Correspondent banking (necessary for international trade) also carries risks, because banks must ensure that their correspondents' due diligence procedures meet appropriate standards. Other areas of corporate banking are probably subject to lower potential threat. Low-threat areas include real estate, investment banking, and payroll services (although these should not be excluded from general scrutiny, because they carry their own financial crime risks).

The financing-of-proliferation threat to other types of banking activities should also be considered. For example, although the threat to retail banking activities is probably low, it is not negligible. Project Alpha's typologies report includes cases of individual customers' using their personal banking facilities to purchase items that violated sanctions or export controls and may have been associated with WMD programs. Nonetheless, the overall financing-of-proliferation threat to private banking is low, because it does not involve industrial activities or international trade.

Countries' vulnerabilities to financing of proliferation are not confined to the formal banking sector. Depending on the products and services they offer, nonbank financial institutions may also be exposed to financing-of-proliferation risks. Table 2 sets out some potentially exposed institutions, although not every financial product or service offered by these institutions necessarily carries a high risk.

Monitoring and Updating Financing-of-Proliferation Risk Assessments

Like all risk assessments, financing-of-proliferation assessments require regular monitoring and updating. For example, several cases in Project Alpha's typologies report involved small companies that changed their type of business as they became involved in proliferation-related activities. The frequency of monitoring depends on individual customers' risk profiles and individual banks' risk appetites; in most financial institutions, the frequency of customer monitoring currently stands at about once a year for high-risk customers, once every three years for medium-risk customers, and, perhaps, once every five years for low-risk customers.[26] Arguably, a high-financing-of-proliferation-risk customer should be monitored more frequently, perhaps on a quarterly basis.

Figure 4: Examples of customer due diligence considerations in understanding financing-of-proliferation risks.

Financial Institutions' Risk Assessments

Financial institutions should incorporate financing-of-proliferation factors into the full range of their internal procedures, systems, and controls. This process should mirror the integration of money-laundering, terrorist-financing, and sanctions factors. And, just as they do with other illicit-financing risks, financial institutions need to educate their staff in financing-of-proliferation risk. Staff members need a basic understanding of the framework of controls on financing of proliferation, of sanctions screening, of screening of equipment and materials if appropriate and where possible, and of typologies and circumvention techniques. They also need to know where to find further information if necessary.[27]

Customer Risk

The first line of defense against financial crime risks in most banks is customer due diligence at the onboarding stage. Customer due diligence should be extended to financing-of-proliferation risk. Once a bank has assessed customer risk, it can restrict the sale of certain products (e.g., trade financing services) accordingly. The U.N. Panel on North Korea has highlighted the crucial importance of effective customer due diligence to detecting attempts to circumvent financial sanctions on North Korea.[28]

Most regulators already require financial institutions both to know and to verify the identity of each customer and to monitor customer activities to detect changes or unusual behavior.[29] Therefore, adding checks for financing-of-proliferation risk to existing due-diligence processes should be relatively straightforward. Financial institutions already assess customer money-laundering or terrorist-financing risk on the basis of considerations such as customer demographics, customer business or activity, status of principals (in the case of an entity or legal person), and the banking products they utilize. To assess financing-of-proliferation risk, financial institutions need to assess to what degree these considerations are vulnerable to financing-of-proliferation threats (Figure 4). Identification of these threats is straightforward; for the purposes of this paper they can be considered equivalent to the indicators listed in Annex 1. Many of these indicators are relevant to customer due diligence, but others may be relevant to different areas of a bank's activities. Checks should extend to negative news screening (for example media of other open source information regarding export-control or related violations).

Customer Demographics

Analyses of customers should take into account customer location, country of incorporation, and location of operations; countries such as North Korea, Iran, Syria, India, Pakistan, and other proliferation-concern countries represent high risk. Customer demographics should also take account of geographies of concern: intermediary countries or regions used by proliferation networks to hide the origin of WMD financing or the destination of materials and equipment procured overseas. Such areas may have weak export controls or financial regulation, may be near countries with WMD programs (e.g., Liaoning Province in China, next to the North Korean border), or have political or historical links with countries with WMD programs. Diversion-concern countries may even have strong export controls but at the same time may have a large diaspora population (from, e.g., Pakistan), which could facilitate the organization of proliferation networks.

A number of published indices are used by financial institutions to assess general country risk, such as Transparency International's Corruption Perceptions Index. However, only one published index is currently available for financing of proliferation, the Peddling Peril Index.[30] This index ranks countries on the basis of ability to prevent proliferation financing, as determined by a comprehensive comparison of FATF and other data.

Status of Individual Customers or Business Principals

As part of the customer due diligence onboarding process, financial institutions should carry out rules-based checks to determine whether names or other details (e.g., address, telephone number, IP address, etc.) match a party on U.N., U.S., EU, or other WMD-related sanctions lists. Sanctions checks should extend to parties that are owned or controlled by designated parties or are acting on behalf of, or at the behest of, designated parties.

The Project Alpha report includes several cases of financing of proliferation involving customers who are dual nationals of countries of proliferation or diversion concern, so financial institutions should factor such customers into their financing-of-proliferation risk assessments. Financial institutions should also factor in negative news.

Customer Business Type or Activities

Certain customer business types or activities are particularly high risk. Manufacturers or suppliers of industrial materials, particularly dual-use goods, are potentially high risk because WMD programs need such goods. Some trading companies are similarly high risk. (Small trading companies, some family-run, are featured in several of the cases in the Project Alpha report.) Universities may be a risk, because scientific research departments could be used as fronts for procuring or funding equipment or materials for WMD programs. Universities with nuclear physics or related technical departments were involved in ordering or paying for goods in some of the cases in the Project Alpha report. Some universities or certain members of staff were designated under U.N. and other sanctions on Iran.

Certain customer business types or activities are particularly high risk. Manufacturers or suppliers of industrial materials, particularly dual-use goods, are potentially high risk because WMD programs need such goods. Some trading companies are similarly high risk.

Banking Products Used by Customer

Transactions associated with WMD procurement look like transactions associated with licit international trade. They both make use of trade finance or open account payments. Although both of these are vulnerable to financing of proliferation, the risk from trade finance is probably lower than that from open account payments. In trade finance, banks require additional documentation, including details of counterparties, consignees, or shipping information. In principle, financial institutions can use this information to conduct a higher degree of due diligence over the transaction as a whole. By contrast, the information accompanying open account transfers (or wires) relates mainly to the financial transaction itself and the parties involved. There is very little information relating to the underlying purpose or nature of the transaction.

Other Areas of Financial Institution Activity That May Carry Financing-of-Proliferation Risk

Financial institutions may also incur financing-of-proliferation risks through their business with correspondent banks and through their customers' counterparties.

There is currently no consistent guidance on managing correspondent bank risks. Under Wolfsberg Group guidelines, financial institutions are simply required to satisfy themselves that they are "comfortable" doing business with a correspondent bank. In doing so, they must take into account that bank's risk profile, the nature of the business relationship, and the regulatory environment.[32] These principles, at a minimum, should be applied to financing-of-proliferation risk. Financial institutions need to assess their correspondent banks' financing-of-proliferation-risk policies and procedures to decide whether these meet their own risk appetite. A correspondent bank's vulnerability to financing of proliferation may depend on its individual customers, and although the Wolfsberg guidelines do not extend to that level, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) has recently created new requirements. FinCEN's 2018 action against a Latvian bank requires financial institutions to implement special due diligence to identify use of their correspondent accounts to process transactions involving that bank (a process known as "nesting").[33]

To assess the financing-of-proliferation risk represented by counterparties (i.e., the recipients or initiators of wire transfers with customers), financial institutions can screen against sanctions lists and check for money-laundering risks. However, a full financing-of-proliferation risk assessment will probably not be possible because of the limited information attached to wire transfers. In these cases, the financial institution should determine a policy based on any financing-of-proliferation information available elsewhere in the organization, such as trade finance or financial investigations units, or from an open source or even the customer itself. In such situations, information shared by government departments may be key.[34]

An Indicative Scorecard for Financial Institutions' Financing-of-Proliferation Customer Risk

Capturing full customer details during onboarding and subsequently monitoring customer activities and profile are crucial to mitigating financing-of-proliferation risk. Table 4 sets out a possible way to quantify customer risk that allows institutions to compare individual customers with peers and monitor them over time. Customers are assigned scores against different possible financing-of-proliferation threats that might apply to them. The scoring system is indicative; financial institutions will need to adapt the details to fit their business and risk appetites. Financial institutions will also need to decide a threshold score, which, if exceeded, will trigger investigations to determine whether further action is needed, including submitting reports to regulators or law enforcement authorities. An institution's business experience and risk appetite will dictate its threshold score.

Annex 2 includes a hypothetical case study to illustrate this scoring system.

Following Up on the Results of Financing-of-Proliferation Risk Assessments[35]

Authorities should incorporate results of financing-of-proliferation risk assessments in national assessments of money-laundering and terrorist-financing risks and disseminate them accordingly. They should take action to mitigate the risks. They should strengthen legislation or regulations if necessary. They should ensure law enforcement and intelligence agencies, and other responsible government departments, are given proper resources to deal with the identified financing-of-proliferation risks.

The results of financing-of-proliferation risk assessments should be shared with other jurisdictions both in the region and elsewhere. These jurisdictions can then take the results into account when carrying out their own financing-of-proliferation risk assessments. This process will help to ensure that countries adopt a consistent approach to assessing financing-of-proliferation risk as well as a shared assessment of measures to combat the threat.

By implementing proliferation-financing risk assessments, financial institutions can demonstrate to regulators, shareholders, customers, and other stakeholders that they are in compliance with or exceeding regulatory expectations. The actions that financial institutions take as a result will depend on legal requirements and corporate practices. In the case of possible matches with parties on sanctions lists, for example, a financial institution will need to comply with the requirements of its host jurisdiction. It may have to halt relevant transactions, freeze assets, and inform authorities. In turn, the authorities may need to inform a relevant U.N. body.

In the case of a suspect customer or transaction identified following a financing-of-proliferation risk assessment, a financial institution could suspend a transaction or customer relationship for internal investigation. It could also seek guidance or additional information from relevant authorities. To the extent that legal constraints and requirements for privacy and data protection allow, as much information as possible should be shared with authorities and with other financial institutions, to facilitate collective action to combat financing of proliferation.

By implementing proliferation-financing risk assessments, financial institutions can demonstrate to regulators, shareholders, customers, and other stakeholders that they are in compliance with or exceeding regulatory expectations.

Conclusions

Wide-ranging and increasingly restrictive U.N. and U.S. financial sanctions attest to the focus of the international community in recent years on the financing of North Korea's WMD program. Financial sanctions were an important component of international controls (implemented by the U.N. and individual countries) on Iran's prohibited nuclear program and (as implemented by individual countries) on Syria's chemical weapons program. Financial controls also play a role in measures to control exports to India and Pakistan's WMD programs.

Although governments and financial institutions must take individual responsibility for implementing controls, combating proliferation financing is ultimately a joint endeavor. An effective control regime requires a series of public-private partnerships, played out at the international, national, and private-sector levels. This effort must join measures to protect national security and measures to control financial risk. To aid this project, policymakers will have to offer a better definition of financing of proliferation and put in place better international controls. However, risk assessments at the governmental and financial institution levels are at the heart of the process.

Financial institutions should be proactive in developing their defenses against financing of proliferation. They should first carry out financing-of-proliferation risk assessments. Although the nature of the financing-of-proliferation threats is different, the principles underlying a strategy to counter them are similar to those for strategies to combat money laundering and terrorist financing; a WMD-proliferation-financing risk assessment should build on existing procedures. Financial institutions should closely coordinate financing-of-proliferation risk assessments with other risk assessments. As with other assessments, they should regularly review them, taking account of changes in products, customers, and the geopolitical environment.

Financial institutions should incorporate financing-of-proliferation factors into the full range of their internal procedures, systems, and controls. Financial institutions need to educate their staff in financing-of-proliferation risk. Staff members need a basic understanding of the framework of controls on financing of proliferation, of sanctions screening, of screening of equipment and materials if appropriate and where possible, and of typologies and circumvention techniques. They also need to know where to find further information if necessary.[37]

By implementing WMD-proliferation-finance identification and risk-assessment procedures, financial institutions can demonstrate to regulators, shareholders, customers, and other stakeholders that they are fully in compliance with or exceeding regulatory expectations. These efforts are good for their reputations and good for their businesses.

Identifying and disrupting the financing of WMD proliferation is unlikely to halt a well-developed WMD program. However, by implementing effective controls to identify the financing of WMD proliferation, financial institutions can support efforts by governments and the international community, and thus contribute to global peace and security.

Table 4: Categorization of Customer Financing-of-Proliferation Risk

Rules-Based Criteria	
Sanctions List	Name match or other match (e.g., address, telephone number) with a party on a sanctions list (i.e. a designated party) or with a record of export-control or related violations. ↳ A financial institution should consider reporting any match to authorities (perhaps as a suspicious-transaction or suspicious-activity report).
	Name match or other match (e.g., address, telephone number) with a party acting on behalf or at behest of, or owned and controlled by, a designated party. ↳ A financial institution should consider reporting any match to authorities (perhaps as a suspicious-transaction or suspicious-activity report).

Table 4 (Continued)

Risk-Based Criteria				
		High Risk (Score 3)	**Medium Risk (Score 2)**	**Low Risk (Score 1)**
Country Risk Factors The Customer is Based in a Country …	That is a WMD proliferator or has a record of being one (A1)	North Korea, Iran, Syria, India, Pakistan	Other countries that might have undeclared WMD programs, according to reliable information (open source or government source)	The rest
	That is of diversion concern (A2)	UAE, Turkey, Iraq, China, Hong Kong, Taiwan, Malaysia, BVI, other countries at high risk of diversion	Singapore, Malaysia, Jordan, Oman, other countries at moderate risk of diversion	The rest
	That hosts a financial or trade center (possibly with weak controls on ML/TF, or weak enforcement) (B13)	Dubai, Turkey, Hong Kong, BVI, Singapore, other countries with high risk of exploitation	UAE, Malaysia, Taiwan, other countries at moderate risk of exploitation	The rest
	That is characterized by a large diaspora from a state of proliferation concern	Dubai, China, Turkey, other countries with large diasporas and relatively weak regulations	Australia, Sweden, U.S., Norway, other countries with large diasporas but relatively strong regulations[36]	The rest
Customer Business Risk The Customer's Business Sector is …	Trading	A small trading company dealing with dual-use goods (B2)	A small trading company dealing with standard industrial goods	Not a small trading company, or a small trading company dealing with non-industrial goods
	Manufacturing	A manufacturer of dual-use goods with a record of export-control violations	A manufacturer of dual-use goods (B3)	Not a manufacturer of dual-use goods (B3)
	Academic and Research	A university (B8) with a nuclear physics or related technical department with history of violations of sanctions or export controls, or designated under sanctions regimes, or members of staff designated under sanctions regimes	A university (B8) with a nuclear physics or related technical department	Another university or not a university
Other Customer Risk Factors The Customer has …	Connections with …	A proliferating country (e.g. dual nationals) (A7)	A country of diversion concern (e.g., dual nationals)	No countries of proliferation or diversion concern
	A pattern of activity that is …	New and inconsistent with business profile (A3)	Occasionally distinct from normal business	Not distinct from normal business (or the company is newly established)
	Customer anti-money laundering/countering financing of terrorism (AML/CFT) controls or compliance procedures that are …	Nonexistent	Weak (B12)	Strong (or the company is newly established)

Alphanumeric references in parentheses are to entries in the table in Annex 1.

Annex 1

List of Indicators of Possible Financing of Proliferation[38]

This is a list of indicators that should be investigated because they may be the result of illicit financial activity. The list is divided into three categories: indicators potentially highly indicative, indicators potentially moderately indicative, and indicators only potentially weakly indicative of financing of proliferation. Indicators that fall into the first category are more likely to indicate financing of proliferation, whereas those that fall into the last category may well reflect other types of illicit activity (e.g., trade-based money laundering). The indicators vary in scope and degree, reflecting the variety of case studies from which they are derived. Countries and financial institutions may be vulnerable to relatively many or relatively few of these indicators, depending on geography, trade links, type of business, and the many other factors discussed in this paper.

Trade-Related Transactions Potentially Highly Indicative of Financing of Proliferation	
A1	Involvement of individuals or entities in foreign country of proliferation concern
A2	Involvement of individuals or entities in foreign country of diversion concern (e.g., a neighboring country or country actively engaged with a country of proliferation concern)
A3	Individuals or entities involved (e.g., customers, counterparties, end users) or their details (e.g., addresses, telephone numbers) similar to, or possibly connected to, parties listed at the time under WMD-related sanctions or export-control regimes, or with a history of involvement in export-control contraventions
A4	Presence of items controlled under WMD export-control regimes[39] or national control regimes
A5	Activity that does not match customers' or counterparties' business profiles, or end-user information that does not match end user's business profile
A6	End user not identified (e.g., a freight-forwarding firm or bank listed as consignee or final destination)
A7	Involvement of an individual connected with a country of proliferation concern (e.g., a dual national), possibly dealing with complex equipment for which he/she lacks technical background
A8	Order for goods placed by firms or individuals from foreign countries other than the country of the stated or suspected end user
A9	Use of cash in transactions for industrial items
A10	Transaction that involves shipment of goods incompatible with the technical level of the country to which it is being shipped (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry)

Trade-Related Transactions Potentially Moderately Indicative of Financing of Proliferation	
B1	Involvement of front companies or shell companies (i.e., companies that do not have a high level of capitalization or display other shell company indicators such as absence of online or physical presence)
B2	Involvement of a small trading, brokering, or intermediary company (possibly carrying out business inconsistent with its normal business)
B3	Customer that is a manufacturer/dealer in products that are subject to export controls
B4	Pattern of transactions of a customer or counterparty, declared to be a commercial business, suggest it is acting as a money-remittance business[40]
B5	Transactions between companies on the basis of "ledger" arrangements that may minimize the need for international financial transactions[41]
B6	Customers or counterparties to transactions that are linked (e.g., they share a common physical address, IP address or telephone number, or their activities may be coordinated)
B7	Transaction that demonstrates links between representatives of companies exchanging goods (e.g., same owners or management)
B8	Involvement of a university in a country of proliferation concern
B9	Description of goods on trade or financial documentation that is nonspecific or misleading
B10	Evidence that documents or other representations (e.g., relating to shipping, customs, or payment) are fake or fraudulent
B11	Use of personal account to purchase industrial items
B12	Transaction that involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export-control laws or weak enforcement of export-control laws
B13	Circuitous route of shipment (if available) and/or circuitous route of financial transaction, possibly through jurisdictions with weak financial regulation or enforcement
B14	Transaction that involves shipment of goods inconsistent with normal geographic trade patterns (e.g., the country involved does not normally export/import the goods involved)
B15	Trade-finance transaction that involves shipment route (if available) through country with weak export-control laws or weak enforcement of export-control laws
B16	Transaction that involves individuals or companies (particularly trading companies) located in countries with weak export-control laws or weak enforcement of export-control laws
Trade-Related Transactions Potentially Weakly Indicative of Financing of Proliferation	
C1	Declared value of a shipment, based on the documentation obtained in the transaction, that is obviously too low vis-à-vis the shipping cost
C2	Inconsistencies in information contained in trade documents and financial flows (e.g., names, companies, addresses, or final destination)
C3	Wire-transfer activity that shows unusual patterns or has no apparent purpose
C4	Customer that is vague or incomplete on information it provides, or resistant to providing additional information when queried
C5	New customer that requests letter-of-credit transaction while awaiting approval of account
C6	Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation

Annex 2: A Case Study

Conducting a Financing-of-Proliferation Risk Assessment

The following hypothetical case is intended to illustrate key points in assessing customer risk.

Bank A, an international bank, is headquartered in a Western country. Bank A has a local branch in an Asian country, Country B. Country B is a regional trade center with commercial and financial links to North Korea and a substantial North Korean diaspora. Because of the existence of these links, Bank A headquarters policy requires that its branches in Country B regularly review customer financing-of-proliferation risk using the categorization in Table 4 (in addition to regular money-laundering and terrorism-financing risk assessments). Bank A checks customers' financial transactions patterns, trade-related documentation, and information held in commercial registries, the media, and the Internet. On the basis of past experience, the bank has set a financing-of-proliferation trigger score of 15. If as a result of the checks a customer exceeds this score, Bank A requires further investigations.

A small local trading company, Company C, recently established itself in Country B. It then opened several bank accounts at Bank A's branch in Country B. The branch carried out standard customer due diligence checks in accordance with Bank A's policy, and determined that the company specialized in the import and export of domestic electrical appliances. Bank A also ascertained that Company C was owned by a family that had emigrated from North Korea some years previously.

None of the details of Company C matched sanctions lists. Using the criteria in Table 4, Bank A assessed that Company C had a customer financing-of-proliferation risk rating of 12. Because this score was below the trigger score of 15, Bank A carried out no further investigations. Instead, in line with its policy, Bank A monitored Company C's transactions and carried out regular reviews.

Bank A subsequently received intelligence from the authorities of the country where it was headquartered. The intelligence stated that Country B was a diversion point for goods and materials shipped illicitly to North Korea's WMD programs.

During a scheduled review of Company C, the bank determined that several factors had changed:

- The company was located in a country now ranked as high risk due to diversion concerns.
- The company was no longer trading only domestic electrical appliances but was now also trading industrial goods and machinery.
- The company appeared to have implemented no compliance procedures.

As a result, Bank A recalculated Company C's financing-of-proliferation rating as 17, which exceeded the trigger score of 15. Bank A therefore carried out further investigations. These determined that since the previous review a year before, Company C had expanded its trade from domestic electrical appliances to include high-grade metallurgical goods, including dual-use goods. Company C was also shipping dual-use goods to companies that, according to media reports, were front companies for North Korea's ballistic missile programs. The shipments were funded through wire transfers from a number of companies located in different overseas jurisdictions.

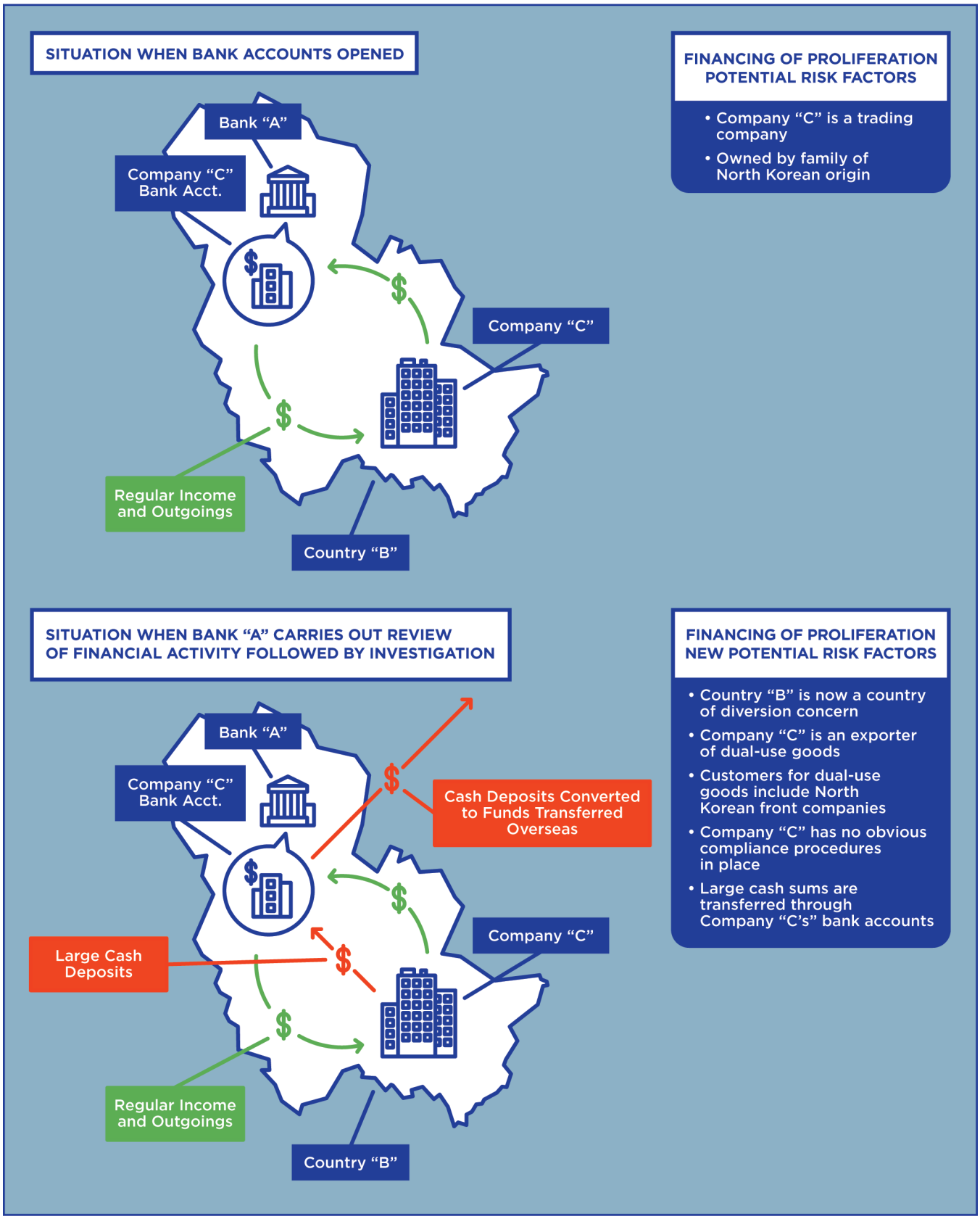
In addition, the investigations showed that the size and frequency of transactions through Company C's accounts had significantly increased and bore no relationship to the company's normal turnover. It appeared that large cash sums were deposited into Company C's accounts and subsequently remitted to trading accounts overseas. The purpose of these transactions was not known (see Figure 5).

Bank A filed a suspicious-transaction report with Country B's authorities, referencing the wire transfers (which it identified as a potential characteristic of financing of proliferation) and the cash deposits. The bank also investigated why its automatic transaction-monitoring programs had not flagged as unusual the unexpectedly large sums Company C was transacting through its bank accounts, amounts not commensurate with Company C's known activities.

Country B's authorities then conducted their own investigations. They noted that the involvement of cash in industrial transactions is a known financing-of-proliferation typology. The authorities prosecuted Company C for export-control violations in regard to shipments of dual-use goods and for providing financial services as a money-remittance business in the absence of a license.

This hypothetical customer due diligence case illustrates the importance of capturing full details during the onboarding process, of subsequent monitoring, and of effective channels of communication with government authorities. The principles apply equally to other areas of a financial institution's activities such as trade finance or correspondent banking. Properly applied, they are crucial to the building of robust defenses against financing of proliferation.

Figure 5: Simplified Illustration of Factors Contributing to Bank A's Assessment of Company C's Financing-of-Proliferation Risk.



Endnotes

1. Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation," (Center for New American Security, January 2018), https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation.

2. Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation."

3. Financial Action Task Force, "Combating Proliferation Financing: A Status Report on Policy Development and Consultation," (February 2010), http://www.fatf-gafi.org/media/fatf/documents/reports/ Status-report-proliferation-financing.pdf. FATF qualifies this definition as a working definition because it is not agreed by the membership as a whole (with some countries concerned that it could include legitimate, non-weapons-related commerce).

4. Although insurance is not specifically mentioned in the definition, insurance providers could also be caught up.

5. Adapted from Table 1 of David Albright, Andrea Stricker, and Houston Wood, "Future World of Illicit Nuclear Trade: Mitigating the Threat," (Institute for Science and International Security July 29, 2013), http://isis-online.org/isis-reports/detail/future-world-of-illicit-nuclear-trade-mitigating-the-threat/.

6. Further information about these countries and programs can be found in studies published by the Institute for Science and International Security (http://isis-online.org); Project Alpha, King's College London (https://projectalpha.eu); and the James Martin Center for Non-Proliferation Studies (https://www.nonproliferation.org).

7. The WMD proliferation network organized by the Pakistani scientist Abdul Qadeer (AQ) Khan in the 1980s and 1990s also used suppliers based in Malaysia, South Africa, Germany, Netherlands, Switzerland, and Turkey.

8. U.N. Security Council Resolutions 1810 (2008), 1977 (2011), 2055 (2012), and 2325 (2016).

9. U.N. Security Council Resolutions 1718 (2006), 1874 (2009), 2321 (2016), 2270 (2016), 2356 (2017), 2371 (2017), 2375 (2017), and 2397 (2017) on North Korea and 2231 (2015) on Iran.

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

11. For example, Singapore (Monetary Authority of Singapore Act and related regulations on Democratic People's Republic of Korea and Iran) and Thailand (Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act 2016).

12. For example, paragraph 192 of the 2012 Report of the UN Panel on Iran created pursuant to resolution 1929 (2010), paragraph 165 of the 2014 Report of the UN Panel on DPRK created pursuant to resolution 1874 (2009), and paragraph 168 of the March 5, 2018 Report of the UN Panel on DPRK created pursuant to resolution 1874 (2009).

13. U.S. Department of the Treasury Under Secretary Sigal Mandelker, speech before the Securities Industry and Financial Markets Association Anti-Money Laundering and Financial Crimes Conference (New York City, February 13, 2018), https://home.treasury.gov/news/press-release/sm0286.

14. According to a banker involved in trade finance, through the International Chamber of Commerce Financial Crime and Policy Group, it was evident that most banks do not have or use lists of prohibited goods.

15. See Page 19, Paragraph 6.1 (a) of "The Wolfsberg Group, ICC and BAFT Trade Finance Principles," http://www.wolfsberg-principles.com/pdf/standards/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.

16. One staff member of an international bank commented that even when a financial institution possessed information about equipment or materials, screening for key words was often difficult. Trade finance documents or payment messages usually referred to brand name or product name. This was generally not the way equipment or materials were referred to on export-control or dual-use-goods lists.

17. Comments by staff members of several international banks late 2017–early 2018.

18. One staff member of an international bank noted that that not all such information provided by governments was available in digital format, and thus easily incorporated into financial institutions' monitoring systems.

19. Financial Action Task Force, "FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment," (February 2013), http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

20. Financial Action Task Force, "Methodology for Assessing Technical Compliance With the FATF Recommendations and the Effectiveness of AML/CFT Systems," (February 2013), http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

21. Financial Action Task Force, "FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment," (March 2013), (http://www.fatf-gafi.org/publications/methodsandtrends/ documents/nationalmoneylaunderingandterroristfinancingriskassessment.html); Financial Action Task Force, "Guidance for a Risk Based Approach: The Banking Sector," (October 2014), (http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf).

22. Financial Action Task Force, "Proliferation Financing Report," (June 18, 2008), http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html; Jersey Financial Services Commission, "Guidance on Proliferation and Proliferation Financing" (October 2011), https://www.jerseyfsc.org/the-commission/proliferation-proliferation-financing/proliferation-proliferation-financing-guidance/; Emil Dall, Andrea Berger, and Tom Keatinge, "Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance," Whitehall Report 3-16, (RUSI, June 2016), https://rusi.org/sites/default/files/201606_whr_3_16_countering_proliferation_finance_v2_0.pdf; Emil Dall, Tom Keatinge, and Andrea Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions," (RUSI Guidance Paper, April 2017), https://rusi.org/sites/default/files/201704_rusi_cpf_guidance_paper.1_0.pdf; David Thompson, "Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System," (C4ADS, 2017), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/59413c8bebbd1ac3194eafb1/1497447588968/Risky+Business-C4ADS.pdf; Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation Final Report," (Project Alpha, October 13, 2017), https://projectalpha.eu/final-report-typologies-of-proliferation-finance/; United States Department of the Treasury, Financial Crime Enforcement Network, "Advisory on North Korea's Use of the International Financial System," (November 2, 2017), https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf; "FCMC in collaboration with U.S. law enforcement authorities identifies weaknesses and imposes monetary fines on JSC 'Norvik Banka" and JSC 'Rietumu Banka,'" Latvian Financial and Capital Market Commission, press release, July 21, 2017, http://www.fktk.lv/en/media-room/press-releases/6479-fcmc-in-collaboration-with-u-s-law-enforcement-authorities-identifies-weaknesses-and-imposes-monetary-fines-on-jsc-norvik-banka-and-jsc-rietumu-banka.html; U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-related Criminal Cases" (February 2017), https://www.justice.gov/nsd/page/file/1044446/download; Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation,"; and Financial Action Task Force, "FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction."

23. Dall, Keatinge, and Berger, "Countering Proliferation Finance: An Introductory Guide for Financial Institutions."

24. See Part III A (ii) of Financial Action Task Force, "FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction."

25. Financial Action Task Force, "FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment."

26. Comment by a member of staff of an international bank, December 2017.

27. See endnote 6.

28. See Paragraph 166 and Recommendation 2 of U.N. Security Council, "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," S/2018/171 (2018), http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2018_171.pdf.

29. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "FinCEN Advisory: Customer Due Diligence Requirements for Financial Institutions," Federal Register 81, no. 91 (May 11, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf.

30. David Albright, Sarah Burkhard, Allison Lach, and Andrea Stricker, "The Peddling Peril Index (PPI) 2017," (Institute for Science and International Security, January 31, 2018), http://isis-online.org/isis-reports/detail/peddling-peril-index-ppi-for-2017.

31. Ideally such information should be available in national company registries; however, not all national authorities make the information publically available.

32. See paragraph 4 of "Wolfsberg Anti-Money Laundering Principles for Correspondent Banking," (Wolfsberg Group, 2014), https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/8.%20Wolfsberg-Correspondent-Banking-Principles-2014.pdf.

33. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Proposal of Special Measure Against ABLV Bank, AS as a Financial Institution of Primary Money Laundering Concern," *Federal Register 83*, no. 43 (February 16, 2018), https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/proposal-special-measure-against-ablv-bank.

34. For example, FinCEN has named ABLV Bank of Latvia an institution of primary money-laundering concern in connection, inter alia, with "transactions for parties connected to UN-designated entities, some of which are

involved with North Korea's procurement or export of ballistic missiles." "FinCEN Names ABL Bank of Latvia an Institution of Primary Money Laundering Concern and Proposes Section 311 Special Measure," U.S. Department of the Treasury, Financial Crimes Enforcement Network, press release, February 13, 2018, https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and.

35. See further discussion in Financial Action Task Force, "FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction."

36. These countries are classified medium risk because overseas procurement agents prefer to seek equipment and materials from reputable manufacturers in countries such as these in Europe or North America. However, a staff member of an international bank noted that a large number of customers were based in these countries, so that monitoring this category would be difficult in practice.

37. See endnote 6.

38. Based on Table 2 of Brewer, "Study of Typologies of Financing of WMD Proliferation Final Report."

39. The relevant WMD export-control regimes are the Nuclear Suppliers Group (NSG), Missile Technology Control Regime (MTCR), and the Australia Group (AG).

40. A remittance business is one that specializes in transfer of money. A license is usually required.

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

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.