Royal United Services Institute
for Defence and Security Studies

Guidance Paper

Countering Proliferation Finance: An Introductory Guide for Financial Institutions

Emil Dall, Tom Keatinge and Andrea Berger

About this Guidance Paper

This introductory guide is the first of two guidance papers to be produced by RUSI on countering proliferation finance. It is aimed at those financial institutions which have carried out little or no concerted thinking on proliferation finance as distinct from other forms of financial crime. The paper seeks to raise awareness of the risk of proliferation financing and create a baseline policy for mitigating the institution against it.

RUSI's second guidance paper will follow on from this introductory guide.

This study was conducted with generous support from the John D and Catherine T MacArthur Foundation.

The authors would like to thank Dr Jonathan Brewer and Anagha Joshi for their invaluable help and input to this guidance.

Countering Proliferation Finance: An Introductory Guide for Financial Institutions

Emil Dall, Tom Keatinge and Andrea Berger

RUSI Guidance Paper, April 2017

Royal United Services Institute
for Defence and Security Studies

185 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 185 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Published in 2017 by the Royal United Services Institute for Defence and Security Studies.

RUSI Guidance Paper, April 2017.

Printed in the UK by Stephen Austin and Sons, Ltd.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Introduction

DESPITE EXPORT CONTROL measures and international treaties seeking to prevent the further spread of nuclear, chemical and biological weapons and their related delivery systems, proliferators have been able to procure and acquire goods for these programmes with relative ease. International efforts to counter this have typically been devoted to the detection and seizure of physical goods, materials and technologies. However, proliferation efforts rely also on finance to facilitate this illicit trade. Indeed, procurement of sensitive WMD-related goods is made possible by the international financial system. Reports from the UN Panel of Experts on North Korea, for example, have highlighted that Pyongyang is 'using greater ingenuity in accessing formal banking channels' to support illicit activities and WMD proliferation.[1]

The role played by the financial sector in disrupting proliferation finance has received greater attention in recent years. Some governments maintain that financial institutions (FIs) have both the capability to detect, and an obligation to disrupt, financial transactions in support of illicit WMD proliferation. However, government initiatives on countering proliferation finance (CPF) vary widely between jurisdictions, and mixed messages on effective strategies have been passed down from governments and regulators to the financial sector. As a result, many FIs, while they may have certain basic controls in place to counter proliferation finance, 'on the whole do not understand the contemporary realities of the threat they are facing',[2] and are failing to implement adequate internal approaches to counter proliferation finance.

This guidance paper seeks to help equip FIs to better understand and mitigate proliferation financing risks. Due to the multifaceted nature of proliferation, and the ever-evolving evasive tactics used by determined proliferators to circumvent sanctions, the response of FIs needs to be flexible. This handbook provides a range of possible approaches that can be adopted, depending on an FI's individual situation, risk profile and risk appetite. In particular, it is designed to catalyse a discussion on proliferation finance in FIs that have carried out little or no concerted thinking on this subject as distinct from other forms of financial crime.

1. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017, p. 4.
2. Emil Dall et al., 'Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance', *Whitehall Report*, 3-16 (June 2016), p. 19.

I. Understanding Proliferation Finance

COUNTERING THE FINANCIAL flows available to proliferators will obstruct and complicate their procurement of illicit goods and the technology needed for the development of weapons of mass destruction (WMD) capabilities and related delivery mechanisms. Countering proliferation finance (CPF) therefore helps national authorities in wider efforts to counter illicit WMD proliferation and safeguards international peace and security in the long term. Devoting attention to CPF also has a direct business incentive for financial institutions (FIs). Involvement in proliferation financing activities, even when inadvertent, carries great reputational risk for FIs: as part of the Chinpo shipping case (Case Study, page 12), one Singaporean FI was publicly linked to North Korean proliferation activities in media reports.[1] FIs can also face financial penalties for providing services in support of proliferation activities. If FIs work to better mitigate their exposure to proliferation finance risk, they may avoid getting caught up in such activities.

CPF measures are important both from a business perspective and for wider non-proliferation objectives. Still, the conversation around CPF measures is in its infancy within many FIs and warrants greater attention. The first step towards a more advanced conversation on CPF measures is to develop an understanding of the proliferation threat underpinning the need for effective CPF measures, an awareness of the obligations and expectations placed on FIs to counter proliferation finance, and an appreciation of the evasive techniques employed by proliferators to circumvent financial sanctions and access the formal financial system.

Current Proliferation Financing Threats

As mentioned previously, focus on proliferation financing has increased in recent years, although it is by no means a new phenomenon. The concept first gained attention in the early 2000s following revelations that AQ Khan, a former nuclear scientist from Pakistan, was operating a clandestine network which obtained and sold sensitive nuclear goods and technologies to clients including North Korea, Iran and Libya.[2] He relied on a network of front companies throughout the world to complete these trades, and routed financial payments in complex patterns to hide the parties to the transaction. Despite uncovering and disrupting Khan's network, procurement for illicit WMD programmes and its associated financing has not ended.

1. Jennifer Dodgson and Leo Byrne, 'Court Case Reveals Chinpo Shipping's Ties to North Korea', *NK News*, 10 September 2015.
2. Michael Laufer, 'AQ Khan Nuclear Chronology', Carnegie Endowment for International Peace, 7 September 2005.

North Korea poses the most urgent current proliferation challenge. Pyongyang has conducted five nuclear and countless ballistic missile tests, and is carrying out further procurement to develop an increasingly advanced nuclear weapons capability. Research conducted by RUSI shows that North Korea continues to access the global financial system via front companies, joint ventures with foreign firms, and especially Chinese FIs, to obtain critical components and technology from around the world, including Europe and North America. The regime also carries out a number of other illicit activities abroad, including conventional arms' trade and trafficking of sanctioned commodities, which make resources available for their nuclear programme.[3]

These activities rely on extensive networks of businesses (including front companies) and middlemen, arranged in complex corporate and ownership structures to obscure any connection on paper to North Korea. However, while some FIs are convinced they do not maintain any links to North Korean individuals or businesses, and have a policy of not processing payments on behalf of North Korean interests, research has shown that unsuspecting FIs around the world continue to inadvertently support the country's illicit trade activities.

As it relates to Iran, a majority of the international sanctions imposed in response to the country's illicit nuclear programme were terminated following the negotiation of the nuclear agreement with world powers (the Joint Comprehensive Plan of Action, or JCPOA). When sanctions were in place, they helped to increase awareness of Iranian illicit procurement efforts and put pressure on FIs to detect and stop this dangerous trade. However, the JCPOA and the subsequent lifting of sanctions against the Iranian nuclear programme have led to the worrying conclusion by some FIs that Iran no longer presents a proliferation threat.[4] This misperception is highly problematic as it risks diverting attention away from efforts to better understand proliferation finance, and counter it when it occurs. In fact, Iran is still prohibited from pursuing an illicit nuclear and missile programme outside the agreed-upon procurement and licensing framework established under the JCPOA. Should Iran once again seek illicit goods and technology outside agreed channels, any services provided by FIs in support of such procurement would be in breach of the sanctions agreement. In addition, a number of Iranian entities and individuals remain designated under UN sanctions, due to their involvement with Iran's ballistic missile programme.[5] If and when FIs re-engage with Iran post-sanctions, they must develop an awareness of these lingering risks.

Given the body of experience with Iranian illicit procurement, including the first-hand experience of many FIs of Iran's proliferation financing activity, now is an ideal time to consider the lessons learned in order to develop a greater awareness of the specific signatures of proliferation finance.

---

3. Andrea Berger, *Target Markets: North Korea's Military Customers in the Sanctions Era*, RUSI Whitehall Paper 84 (London: Taylor and Francis, 2015).
4. Emil Dall et al., 'Implementing the Iran Nuclear Deal: Balancing Proliferation Finance Risk and Economic Opportunity', *RUSI Occasional Papers* (December 2016).
5. Under the JCPOA, most UN financial sanctions relating to Iran's nuclear programme were terminated, but some individuals and entities connected to Iran's ballistic missile activities will remain under sanctions until at least eight years after implementation of the agreement.

Characteristics of Procurement of Goods

Before advancing a discussion on the financial aspect of proliferation, FIs should strive to understand how the underlying procurement of goods for illicit WMD programmes works. Generally speaking, proliferation can be defined as the illicit spread of WMD capabilities, such as nuclear, chemical or biological weapons, and their related delivery vehicles. However, modern proliferation does not involve the purchase of finished off-the-shelf weapons. Rather than seeking a complete WMD system, most proliferators seek the individual goods and component parts needed for the development of WMD and missile programmes in order to manufacture and develop at home. This way, procurement for their programmes becomes harder to detect as goods are sought from a variety of companies over a longer period of time. Disruption of one shipment is less likely to hinder the overall programme, and the goods are more easily replaceable.

This trend is further complicated by the fact that goods and technology procured do not always appear on one of the international export control lists. It should be noted that even if goods and technologies do not feature on certain international export control lists, they are still subject to export control restrictions if their end use is for illicit proliferation purposes. While certain goods may fall within the threshold determined as 'sensitive' by export control regimes, proliferators have become skilled in procuring goods just below the controls threshold. In fact, the UN Panel of Experts on Iran reported in 2014 that only 10% of the goods that it was investigating fell within the thresholds determined by control lists.[6] Proliferators are becoming more adept at upgrading the technology domestically to the level required for a WMD and missile programme, and have become skilled at manufacturing many components locally. Such a procurement pattern makes it harder for authorities to determine whether procured goods (with a host of benign commercial applications) may eventually be destined for an illicit WMD programme. As it relates to FIs, it cannot be assumed that simply focusing on financial transactions involving controlled items subject to export restrictions will be enough to counter proliferation finance.

Procurement of sensitive goods and technology for illicit WMD programmes is complex, and involves several entities from manufacturing through transport and to final end use. For example, the UN Security Council has previously noted that North Korea 'uses complex, opaque ownership structures for the purpose of violating measures imposed in relevant Security Council resolutions' and the council seeks to 'identify individuals and entities engaging in such practices' to designate them on international sanctions lists.[7]

However, while proliferation may be carried out by individuals and entities found on sanctions lists, this is often not the case. Sanction regimes against proliferating states, such as North Korea, do not cover the full extent of proliferation networks and proliferation activity goes well beyond the entities and persons designated on various sanctions lists. For example, at the time of writing the current UN sanctions regime against North Korea only includes a total of 39

6. UN Security Council, 'Final Report of the Panel of Experts Established Pursuant to Resolution 1929 (2010)', S/2014/394, 5 June 2014, p. 10.
7. UN Security Council Resolution 2270, 2 March 2016, SC/12267, p. 4.

individuals and 42 entities.[8] At the same time, research continues to show that the extent of North Korea's illicit procurement involves a much greater number of actors, partly because of the trend towards blending illegal trade into legitimate commercial business.

Proliferators make use of a network of middlemen and agents located overseas to procure necessary materials. Often it is not immediately obvious that these agents hold any connection to proliferating jurisdictions, and many of them will mix their illicit trade activities with legal trade, making it more difficult for authorities to detect illicit business. Furthermore, proliferators make use of several transhipment points before the goods reach their end destination. Transhipment points, where goods can be relabelled, are a useful way for proliferators to obscure the logistical path, making it almost impossible for authorities, as well as suppliers or shipping companies that believe they are part of a legitimate and legal transaction, to tell the origin or end destination of a shipment. It is certain that procurement will involve false end-users located outside proliferating countries themselves.

It is also difficult for the international community to rapidly add new individuals and entities to sanctions regimes for a number of reasons. First, because of their multilateral nature, some states may object to adding certain entities or individuals to sanctions lists. Second, multilateral sanctions depend on individual countries to implement them, which is sometimes lacking in certain jurisdictions. Third, once an entity or individual is designated for proliferation activities, many will be able to quickly reform their on-paper presence. Proliferators (unless they are middlemen who maintain broader business interests other than just engaging with a proliferating state) will establish new front companies, or change the directorship of existing ones, in order to hide any connection to a now-sanctioned party. Efforts to designate proliferators are therefore often outrun by evasive techniques by proliferators to find new pathways to procure and obtain sensitive goods and technology, rendering designation processes quickly futile in terms of their longer-term disruptive effect.

Still, however, sanctions designations remain important for asset-freezing purposes and to ensure that FIs have the legal tools available to them to hinder designated entities and individuals from using the formal financial system. Designations are also useful in identifying actors central to a country's illicit procurement efforts, and can provide a good starting point for learning more about the wider network of individuals and entities involved with procurement efforts, even if they do not represent the full extent of procurement activities, as mentioned previously.

It is also important to emphasise that proliferation can occur in both directions. For example, while North Korea may be procuring technology from abroad needed for its nuclear programme, it has become adept in manufacturing and constructing related ballistic missile technology domestically. It has also exported these capabilities to foreign buyers, including Syria, Egypt, the United Arab Emirates (UAE), Yemen and Iran. In countering proliferation of WMD capabilities, one should not only consider the flows going into a major proliferating state such as North Korea, but also the sensitive goods it might provide to others. In addition to ballistic missile technology, North Korea has built up a significant portfolio of illicit trade activities on which it

8. UN Security Council Subsidiary Organs, 'Security Council Committee Established Pursuant To Resolution 1718 (2006): Sanctions List Materials'.

depends for income to support its expanding WMD programme. Historically, this has included both the falsification of currency and the illicit trafficking of wildlife and conventional weaponry.

Countering Proliferation Finance: Obligations

Just as the procurement of goods for illicit WMD programmes and their related missile delivery systems is a multifaceted and complex affair, so too is related financing. Proliferators have developed novel ways of operating within the global financial system to evade detection and circumvent increasingly stringent sanctions regimes and CPF regimes.

FIs are subject to a number of obligations relating to CPF. Some of these are established in international law, meaning that governments are responsible for transposing regulations into national law, though global implementation efforts remain highly uneven. Other obligations are enacted purely at the domestic level, and can therefore vary between jurisdictions.

International Obligations

At the international level, since 2012, initiatives to counter proliferation finance have been housed within the Financial Action Task Force (FATF), the global standard-setter on combating financial crime risks. FATF promotes a set of Recommendations which member states are expected to implement within their own jurisdictions.[9] While these recommendations may not create formal obligations, they do provide an assessment framework through which states can be assessed for their efforts in countering financial crime risks. Recommendation 7 is devoted exclusively to CPF, and focuses on the proper and timely implementation of UN-targeted financial sanctions against entities and individuals (see Box 1). Following the termination of most UN targeted financial sanctions against Iran in January 2016, the Recommendation in effect covers only North Korean-designated entities and individuals. While certain Iranian entities and individuals remain designated, this is a small number and only for a limited time period.

Box 1: FATF Recommendation 7.

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

Source: FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', February 2012 (updated October 2016).

9. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', February 2012 (updated October 2016).

While the Recommendation is an important international baseline to counter proliferation finance, it has not altered the obligations in place for FIs which already implement UN sanctions by virtue of those sanctions forming international law. FIs should already be implementing targeted financial sanctions without help from their national governments, and the FATF Recommendation therefore only reconfirms that screening against designated entities and individuals connected to illicit nuclear programmes should be a standard practice of CPF efforts.

In fact, FATF's Recommendation is now increasingly out of touch with other international obligations on CPF. UN sanctions regimes incorporate measures that go beyond list-based sanctions implementation, and focuses to a greater extent on activity-based obligations to counter proliferation finance. For example, current UN obligations as related to proliferation finance and North Korea include the banning of correspondent banking relationships with the country's FIs and a range of other activity-based measures, beyond lists of designated entities. A full list of relevant financial obligations relating to proliferation finance in UN Security Council resolutions is contained in Annex 3.

Another UN measure which is not covered under the FATF regime is Resolution 1540, which was adopted in 2004 in response to concerns that non-state actors would be able to acquire proliferation sensitive goods. Resolution 1540 includes a reference to the financial aspect of procurement efforts, and calls on Member States to criminalise proliferation financing activity in national legislation.[10]

Since then, little work has taken place within the 1540 framework on CPF measures. The 1540 Committee, established to monitor the implementation of the resolution, confirmed in a recent review report that most states make use of penal codes or legislation related to other financial crime risks, rather than adopting dedicated legislation specific to proliferation financing.[11] National governments have received little guidance on how to operationalise CPF commitments under 1540, which is activity rather than list-based, and as a result the obligation has not filtered through to financial institutions.

National Obligations

In addition to obligations at the international level, there are several national requirements which differ between jurisdictions. While all governments agree that FIs should play some role in CPF efforts, they are split over how. There are those who are sceptical that it is possible for FIs to do more than simply screening transactions for designated entities and individuals. Others feel that FIs should play a more active role in detecting and stopping proliferation finance activity beyond sanctions lists. As a result, the reach of proliferation finance obligations at the national level (both those established in law and those communicated informally by governments) differs.

10. UN Security Council Resolution 1540, 28 April 2004, S/RES/1540.
11. UN Security Council, 'Report of the Security Council Committee established pursuant to resolution 1540 (2004)', S/2016/1038, 9 December 2016, p. 23

RUSI has found that certain jurisdictions, such as the US, as well as some European countries, appear to have an expectation that FIs can and should play a very active role in detecting and disrupting proliferation finance. Conversely, other governments object to placing onerous expectations upon their financial sector, which they perceive as unrealistic in practice. Germany, for example, has been reluctant to establish expectations that go beyond screening incoming and outgoing transactions against a list of designated entities and individuals. It was found that 'due to the lack of [other] information contained in payment messages accompanying most financial transactions' this is not a task upon which the government feels that FIs can necessarily embark.[12]

Most FIs operate across jurisdictions and are thus required to take into consideration the obligations and expectations communicated by a range of governments and regulators. They base their approach to sanctions implementation on the highest common denominator of implementation, and work towards expectations set forth unilaterally by the US government, which tend to be stricter in this respect. Among some FIs, this has also resulted in more attention being paid to proliferation finance, recognising the fact that US authorities do feel that FIs have an important role in CPF.

Therefore, even if the home jurisdiction of an FI does not have major expectations in the CPF space, a number of other risks need to be taken into account, including the damage to an FI's reputation resulting from involvement in proliferation financing risk. Any FI with a global footprint will also be concerned about access to the US market. In the US, successive administrations have moved to expand national sanctions regimes against proliferators beyond those provided by the UN, and in turn requirements on CPF. For example, under the USA PATRIOT Act Section 311, jurisdictions may be designated as being of 'primary money laundering concern'.[13] This designation was most recently brought against North Korea in 2016, and gives US authorities the power to penalise any FI that conducts business with a designated jurisdiction, and restricts FIs from operating correspondent bank accounts on behalf of the designated jurisdiction.

It is also important to note that other financial crime risks, such as money laundering and corruption risks, also play a role in causing risk-aversion within many FIs.[14] FIs are also aware of the general business risk involved with engaging with certain jurisdictions. Despite the JCPOA, a number of Iranian entities and individuals remain designated for their involvement in other prohibited activities, such as ballistic missile development or support for terrorist activities. A major concern for many FIs is the Iranian Revolutionary Guards Corps (IRGC), which has an extensive presence throughout Iranian society, including controlling or part-owning many businesses and is still subject to sanctions. FIs need to make sure that they are not providing financial services to or facilitate transfers on behalf of still-sanctioned entities. Furthermore, the

12. Dall et al., 'Out of Sight, Out of Mind?', p. 7.
13. US Department of the Treasury, 'Fact Sheet: Overview of Section 311 of the USA PATRIOT Act', 10 February 2011.
14. Dealing with Iran, even without sanctions, continues to carry exposure to general financial crime risks. Iran has long been identified as one of two (with North Korea) 'high-risk and non-cooperative' jurisdictions with actions put against them by FATF. Iran was ranked as the highest-risk country in the world for money laundering by the Basel Institute on Governance in 2016, and is ranked 113 out of 176 on Transparency International's Corruption Perceptions Index for 2016.

guidance on what FIs are expected to do with respect to companies partly owned or controlled by still-designated organisations, such as the IRGC, is contradictory and uncertain.[15]

When considering the range of obligations they must follow, FIs should therefore take into account the variation in expectations – both formal and informal – between countries, as well as the general risk and exposure to wider financial crime risks they are willing to accept. It should, however, also be noted that an approach that seeks to simply avoid any and all trade with a certain jurisdiction may not necessarily constitute an effective CPF approach. Proliferators are employing increasingly sophisticated methods to hide their connections to jurisdictions of concern. Indeed, without this, North Korea would not be able to move funds through the formal financial system with such apparent relative ease. It is therefore important that FIs understand what proliferation finance looks like in practice, and adopt approaches that move beyond a list-based screening approach.

Countering Proliferation Finance: Practice

Proliferation finance refers to the underlying financial services which make the procurement, shipment and receiving of illicit goods possible.

As the definition in Box 2 states, proliferation finance is more than simply the payment for goods, but involves financial services provided in support of any part of the procurement process, and not directly connected to the physical flow of goods. This is important to note for FIs, which will be expected to detect and counter proliferation finance at all stages where it exists, whether that is a financial transfer used to pay manufacturers, a ship mortgage or credit line for shipment of illicit sensitive goods, insurance services, or middleman fees.

As previously mentioned, proliferation finance obligations exist both at the international and the national level, which FIs must take into account. This includes implementing relevant sanctions regimes as they refer to proliferation finance, including activity-based restrictions on access to the global financial system by proliferators.

15. In light of the complexity of this task, the US recently issued further guidance, stating that non-US financial institutions are not prohibited from conducting transactions with entities that are minority owned or controlled 'in whole or in part' by a still-designated organisation, such as the IRGC. However, the guidance also states that the US 'recommends exercising caution when engaging in transactions with such entities' and warns that 'screening the names of Iranian counterparties against [sanctions lists] … would generally be expected, but that is not necessarily sufficient'. See Dall et al., 'Implementing the Iran Nuclear Deal: Balancing Proliferation Finance Risk and Economic Opportunity', p. 8. Quotes from US Department of the Treasury, Office of Foreign Assets Control (OFAC), 'Frequently Asked Questions Relating to the Lifting of Certain U.S. Sanctions Under the Joint Comprehensive Plan of Action (JCPOA) on Implementation Day', issued on 16 January 2016, updated 7 October 2016, <https://www.treasury.gov/resource-center/sanctions/Programs/Documents/jcpoa_faqs.pdf>, accessed 8 February 2017.

Box 2: FATF Definition of Proliferation Finance.

[T]he act of providing funds or financial services that 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).

Source: FATF, 'FATF Report: Combating Proliferation Financing: A Status Report on Policy Development and Consultation', February 2010, p. 5.

Just as proliferators have used evasive tactics to procure goods and technology for illicit WMD programmes, so they have employed a number of evasive techniques to circumvent the financial sanctions restrictions applied against them, and to access the financial system. FIs should therefore be prepared that the names of designated entities or individuals rarely appear in financial transactions. Proliferators use middlemen, agents located abroad and front companies separated from the actual movement of goods to carry out their financial activities. Entities and individuals involved in transactions may not even have an obvious connection on paper to the proliferating country, or not yet be designated on international sanctions lists. Similarly, even if FIs were to simply screen against nationals from a particular country (for example, North Korea), proliferators have been known to make use of foreign nationals, or nationals who hold dual citizenship in another country, to facilitate financial activities.

Facilitators, such as middlemen, may co-mingle funds used in support of illicit activities with legal business operations. Co-mingling enables proliferating agents to conceal illicit transactions and financial activity amid non-suspicious transactions, and use legal transactions as a cover story for their activities.

Proliferation-financing tends to be directed by state actors, who develop their own networks and distinctive ways of accessing the formal financial system. FIs should therefore be aware, when devising strategies to counter proliferation finance, that proliferation networks directed by the North Korean regime will look different from those operated by Iran.

For example, while the establishment of front companies for the procurement of goods and associated payments can happen throughout the world, there is a particular presence of overseas North Korean business networks operating in China, Hong Kong, Singapore and Malaysia. While these entities do not have a direct connection to designated entities on paper, it is often possible to establish a link between front companies and the bodies that control them by conducting network analysis into connected parties. Proliferation financing risk can therefore be geographic, as proliferators have their preferred access routes to the formal financial system and jurisdictions where they have a particularly strong presence.

North Korea's Use of the Global Financial System

Despite financial restrictions in place, North Korean FIs and their associated networks continue to be able to access the global financial system.

Designated North Korean FIs are known to hold correspondent bank accounts or relationships with foreign FIs in violation of UNSCR 2270. Correspondent banks carry out financial transactions on behalf of their North Korean counterpart, and give North Korea an access point to the wider global financial system. It is believed that North Korea has particularly used correspondent accounts held with Chinese banks to facilitate its international financial transfers. Some Chinese banks also maintain offices or branches within North Korea,[16] though it is possible that this will change following UNSCR 2321, which banned them from doing so.

North Korean FIs are no longer permitted to maintain representative offices or branches abroad. However, despite this restriction, North Korea is known to 'keep assets offshore in accounts that conceal North Korean ownership, and use those assets to facilitate international transactions'.[17] This is particularly true with trading companies operating in the border provinces of Jilin and Liaoning in China. In addition, many of the country's overseas representative missions and embassies are actively involved with illicit trade activities, and process financial transfers on behalf of designated entities in support of proliferation activities.[18] With increasing financial restrictions imposed upon it, North Korea has also devised novel ways of circumventing financial sanctions by withdrawing bulk cash and gold from accounts overseas, before transporting them back home.[19]

It is worth noting that North Korean funds do not need to go back to the country to benefit the regime. In fact, by keeping assets offshore in bank accounts that have no apparent link to North Korea, the regime is able to facilitate their international trade through those accounts.

Other jurisdictions with extensive North Korean business networks include Singapore, Hong Kong and Malaysia, and the regime continues to access the financial system from these bases. For example, a North Korean shipping network in Hong Kong was used for supporting illicit activities and partly financed by major FIs in the region. Similarly, when Iranian procurement activities were at their highest, the country indirectly accessed the global financial system through Turkey and the UAE. In devising their response to proliferation financing risk, FIs should take into account both geographic patterns of different proliferators as well as the proliferating country's other legitimate trade relations, which are often exploited for proliferation financing purposes.

16. Andrea Berger, 'The New UNSC Sanctions Resolution on North Korea: A Deep Dive Assessment', *38 North*, 2 March 2016.
17. *Ibid*.
18. Andrea Berger, 'The 2016 UN Panel of Experts Report: An Eye-Opening Account of Persistent Blindness', *38 North*, 19 April 2016.
19. Jack Kim and Louis Charbonneau, 'North Korea Uses Cash Couriers, False Names to Outwit Sanctions', *Reuters*, 16 February 2013.

Case Study: Chinpo Shipping (Private) Limited[20]

In July 2013, Panama Canal authorities detained a North Korean vessel, the *Chong Chon Gang* (CCG), while it was transiting from Cuba to North Korea. Canal authorities found a shipment of arms and related materials concealed under other cargo.[21] The CCG was operated and managed by Ocean Maritime Management Company Ltd (OMM), one of the largest North Korean shipping companies.[22]

Some of the costs connected with the voyage of the CCG were paid by Chinpo Shipping Company (Private) Limited, based in Singapore. Following investigations, Singapore authorities filed criminal charges, and Chinpo was convicted of financing proliferation[23] in connection with $72,016.76 that the company had remitted by wire transfer from a Bank of China account[24] to a Panama Canal shipping agent.[25] Chinpo was also convicted of carrying out an unlicensed remittance business.

According to court documents,[26] Chinpo Shipping Company (Private) Limited was a ships' agency, chandlers and general wholesale importer/exporter. It was one of three companies run by a Chinese family who shared the same business address, employees and an email account for communications with North Korean entities. They also shared an account at the Bank of China (in Chinpo's name). The North Korean Embassy in Singapore used the business as a postal address. Separate accounts held by Chinpo with Union Bank of Singapore and International Commercial Bank had been closed by those financial institutions years earlier because of suspicious transactions. It is unclear whether North Korean officials in Singapore were given access to those accounts when they were open.

Chinpo had had business relationships with North Korean shipping companies since the 1980s and with OMM since the mid-1990s. Chinpo hosted OMM staff at its offices and used its Bank of China account to manage funds on behalf of OMM. Monies due to OMM (for example, freight charges) were paid into the account. Monies were remitted from the account at OMM's request, for example to North Korean vessel owners (who were not able to set up their own bank accounts because of sanctions), or on their behalf for supplies, port charges or other disbursements, or from one North Korean ship owner to another. Chinpo also used the account to transfer funds to OMM.

20. This case study was put together with help from Dr Jonathan Brewer, visiting professor at King's College London, RUSI Associate Fellow and Adjunct Senior Fellow at the Center for a New American Security, Washington, DC.
21. The arms and related materials included two MiG-21 jet fighters, anti-tank rockets, and SA-2 and SA-3 Russian-made surface-to-air missile systems and their components.
22. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2014/147, 6 March 2014.
23. The specific charge was 'transferring financial assets or resources that may be reasonably used to contribute to DPRK's nuclear programmes or activities'.
24. Account No. 002963-7510-014.
25. Public Prosecutor vs. Chinpo Shipping Company (Private) Ltd [2016] SGDC104. Specifically, the judge concluded that the arms and related material onboard the vessel could contribute to North Korea's overall nuclear capability, and thus the payment of $72,106.76 for transit fees through the Panama Canal was in connection with North Korea's nuclear capability.
26. Public Prosecutor vs. Chinpo Shipping Company (Private) Ltd [2016] SGDC104.

Chinpo kept track of these funds on OMM's behalf, and they were separate from Chinpo's chandelling and ship agency services. Over three years, 605 remittances took place, totalling more than $40 million, all related to North Korean vessels. Chinpo was effectively operating as a remittance business, although it had no licence to do so from Singapore authorities. Once a year, a North Korean diplomat with access to the Chinpo account would withdraw up to $500,000 in bank notes to carry out of the country. She was stopped on only one occasion by the Singaporean authorities.[27]

Chinpo tried to hide its involvement with North Korean companies by removing the names of North Korean vessels and other identifying details from remittance forms and email correspondence, allegedly at a Bank of China teller's recommendation. Payments from Chinpo's account took place in the absence of invoices or other details.

The court documents record that the Bank of China queried a remittance by Chinpo on only one occasion. In connection with payment for expenses regarding the outward of leg CCG's voyage to Cuba, the bank requested details of the ship's cargo, its consignee in Cuba, and the bill of lading. These details were provided. Bank of China closed the Chinpo account in 2013.

Had additional financial crime, due diligence and 'know your customer' steps been taken by Bank of China, they may have encountered important red flags at an earlier stage. Chinpo's chandelling business was solely for North Korean ships, which should have automatically put the company in a high-risk category. A sudden change in practice by Chinpo to non-declaration of the vessels involved in transactions should have been met with concern, as should regular withdrawals of bulk cash by a Singapore-based North Korean diplomat. As the prosecutor in the case noted, prudent anti-money-laundering procedures by the Bank of China could also have highlighted the irregularity of the account activity in the context of Chinpo's declared business.[28]

27. Sangwon Yoon et al., 'How North Korea Funnels Cash Into the Country', *Bloomberg*, 22 February 2016.
28. *Ibid.*

Key Points:

- Countering proliferation financing is key to obstructing efforts of proliferating states to procure goods and technology needed for their illicit WMD programmes. North Korea poses the most urgent current proliferation challenge.
- Proliferators seek individual goods and component parts which may not always appear on international export control lists. In addition, sanction regimes against proliferating states, such as North Korea, do not cover the full extent of their proliferation activity, which extends well beyond the entities and persons identified on sanctions lists.
- Proliferation finance encompasses more than simply the payment for goods, but involves financial services provided in support of any part of the procurement process, and not directly connected to the physical flow of goods. Proliferators make use of middlemen, agents located abroad, co-mingling of licit and illicit activities and front companies separated from the actual movement of goods to carry out their financial activities.
- Correspondent banks carry out financial transactions on behalf of their North Korean counterpart, and give the country an access point to the wider global financial system. It is believed that North Korea has particularly used correspondent accounts held with Chinese banks to facilitate its international financial transfers.
- Therefore, even if financial institutions are convinced they do not maintain any links to North Korean individuals or businesses, they may still be inadvertently supporting North Korean procurement activities.
- When considering the range of obligations they must follow, FIs should take into account the variation in expectations – both formal and informal – between countries, as well as the general risk and exposure to wider financial crime risks they are willing to accept.

II. Building Blocks for an Effective Response to Countering Proliferation Finance

SUCCESSFULLY COUNTERING PROLIFERATION finance necessitates an approach which considers the complex nature of proliferation, as well as the unique risk profile and appetite of individual FIs. This guidance offers a number of different considerations that may be adopted by FIs to further their internal policies to move beyond simply a list-based screening approach and develop the first building blocks towards a more advanced response to proliferation financing threats.

Proliferation finance covers implementation of sanctions regimes put in place by all governments. It can therefore be assumed that all FIs are already committed to basic screening against UN sanctions lists related to proliferators, currently against North Korea and the remaining restrictions on Iran. This will involve the use of software to screen all incoming and outgoing transactions against lists of entities and persons designated under international sanctions regimes. All FIs will already be screening UN lists for this purpose, while many others are also implementing sanctions lists issued by the US and the EU which often go beyond the designations made at the UN level. Most FIs use third-party providers of screening software, with whom they work should closely to make sure that the software corresponds with their unique risk appetite.

However, as the previous section made clear, the full extent of proliferation financing activity will extend far beyond those entities and individuals found on sanctions lists. As a result, it is necessary for FIs to devise strategies to mitigate proliferation financing activity which also go beyond a list-based screening approach to CPF.

Many FIs have made assessments about the risk they are facing from other forms of financial crime, such as terrorist financing or money laundering. An internal risk assessment is carried out to determine exposure to a certain financial crime risk, and what measures could be put in place to mitigate the risk. Similar efforts are often lacking when it comes to proliferation finance.

The starting point for advancing internal strategies on CPF should therefore begin with an assessment of the exposure of the FI to the risk at hand. Such a risk assessment will also help FIs to determine what level of risk they are willing to accept, and whether any existing or new business relationships fall outside this spectrum. This section will help towards that effort.

Countering Proliferation Finance as a Distinct Financial Crime Risk

Many FIs have currently made more progress in their thinking on counter-terrorist financing (CTF) and anti-money-laundering (AML) efforts. They have had many years to develop awareness and adequate responses to these types of financial crime risks, and they are also the risks which tend to receive the greatest amount of attention from governments. As a result, typologies for CTF and AML are more developed, detailed and accessible for FIs.

In cases where typology reports are issued specifically on proliferation finance, they still tend to share several characteristics of AML and CTF typology reports. As a result, some FIs currently believe they are already catching proliferation financing simply by continuing to implement their strategies related to CTF and AML.

While it is true that proliferation financing activity may share certain characteristics with other forms of financial crime, and therefore one avenue to detect it is to use strategies developed for other financial crime risks, this ignores some of the characteristics which are unique to proliferation finance trends. As a result, detection mechanisms informed by CTF and AML may fail to detect proliferation finance activities.

Unlike other financial crime risks, such as money laundering and terrorist financing, of which FIs have greater experience and knowledge, proliferation finance tends to be directed by state actors, such as North Korea and Iran. This is an important feature that can make proliferation finance distinct from other types of financial crime. As a consequence, proliferation networks directed by the same country tend to behave similarly. This can include the jurisdictions used for establishing overseas business networks and front companies, the preferred suppliers of goods, or evasive techniques. This should be kept in mind by FIs as they devise CPF strategies.

Identifying Suspicious Transactions

As previously mentioned, proliferation financing activity is not limited to individuals and entities designated on sanctions lists. Proliferation financing activity may involve other actors with no immediately obvious connection to designated entities and individuals, and can be disconnected from the physical flow of proliferation-sensitive goods.

Over the years, a number of ‘indicators’ of proliferation financing activity has been put into the public space by international organisations and governments. These indicators are meant to provide FIs with a toolkit to better identify potentially suspicious transactions, although they vary in their degree of usefulness and specificity. During its review of available indicators and

guidance on identifying proliferation financing activity, RUSI found that a number of issues should be kept in mind by FIs before they implement these indicators into their internal practices.[1]

Many publicly available typologies on proliferation financing are based on indicators developed to counter other forms of financial crime. Some overlap between proliferation financing activity and other financial crime should be expected, as proliferators will inevitably employ tactics used in other areas of financial crime. However, by relying exclusively on this overlap, the specific features that are specific to proliferation finance is neglected.

This means that some FIs have had some success in successfully identifying suspicious transactions connected to proliferation financing by relying on indicators and red flags available in the public domain. However, it is not always clear to the FI whether all activity is being caught by relying on guidance devised to counter other forms of financial crime.

A separate issue has to do with technical expertise. Certain indicators are difficult for FIs to action, either because of a lack of information or a lack of training and resources. FIs should therefore determine whether they have the internal technical capability to implement all indicators, and where possible provide training for its staff to heighten their technical expertise in these areas. Certain indicators are difficult for FIs to action, either because of a lack of information or lack of training and resources.

The appearance of a red flag does not automatically make a transaction suspicious. For example, if the transaction involves a country of 'diversion' concern (for example, China), it should not automatically be classified as proliferation finance. However, when combined with other potential indicators of proliferation finance, such as a circuitous payment trail or a company which appears to be a front company, FIs should aim to conduct a deeper investigation into such transactions.

Annex 2 contains a list of indicators and red flags as supplied by FATF, as well as reference to other indicators to provide further context to help FIs address these red flags. It should be noted that many available indicators focus on trade-based money laundering, rather than proliferation financing risk specifically.

While some of these indicators may not be feasible for some FIs to carry out, it should be up to the individual FI to determine which indicators it wishes to implement internally in its screening processes, and which indicators adequately addresses the unique risk profile of the institution. These indicators are contained in Annex 2.

1. Previous RUSI research has found that twelve of the 20 indicators of proliferation identified by FATF had already been included in other forms of guidance produced by them, and eighteen were featured in other financial crime guidance. See Dall et al., 'Out of Sight, Out of Mind?', p. 16.

Focusing on Particular Proliferators and Areas of Operation

FIs may choose to focus on their exposure to specific proliferators, including their preferred tactics in circumventing sanctions and their geographical areas of operation. This way, FIs may determine whether the institution carries out business which may be exposed to these operations. A good starting point for learning more about specific proliferation actors, in particular North Korea, is the UN Panel of Experts reports, which provides detailed information on North Korea's procurement patterns and geographical areas of operation. Financial institutions may consider the following as part of this effort:

1. The institution should consider its individual risk situation as it relates to a particular proliferator.

FIs should take stock of current proliferation threats and become familiar with the tactics used by different proliferators. For example, when it comes to determining risk exposure to North Korean proliferation finance activity, FIs should clarify their policy on maintaining relationships with foreign banks, businesses or individuals who continue to have business ties with North Korea. Banks in China should warrant particular consideration, given the volume of direct and indirect North Korean business that flows through that country. As previously stated, North Korean middlemen and overseas networks often mix their illicit procurement activities with legal trade, thus making it difficult to distinguish between the two. FIs should consider the risk factor of clients involved in legal trade, but may indirectly be caught up in illicit activity by extension of their affiliation with a proliferation network directed by a proliferating state. For example:

- Does your institution have clarity over whether any clients or correspondent banks located in China or other exposed jurisdictions maintain active links with North Korea?
- Has your institution determined whether client relationships will be maintained with middlemen who facilitate legal trade with North Korea?

2. The institution should determine the extent of its operations in jurisdictions where proliferators are known to operate.

By studying the trends and tactics used by proliferators, FIs can focus on a few jurisdictions in which proliferation networks operate. If it is North Korea, the FI should focus on the locations where the country maintains large corporate networks. An FI with substantial business in China, especially with provinces that border North Korea, will almost certainly be exposed to North Korean business. FIs should also consider their relationships with correspondent banks in those jurisdictions, and clarify with their partners how they address North Korean business. For example:

- Does your institution have correspondent banking relationships with FIs in China that have significant business in the border provinces (Liaoning and Jilin)?
- Does your institution have significant business in the provision of shipping insurance? North Korean shipping is the subject of significant stringent sanctions in order to stem logistical opportunities for proliferation.

Building on a List-Based Screening Approach and Knowing Your Customer

Appreciating the fact that proliferators establish complex procurement networks to cover their tracks and conceal involvement in a particular financial transaction, FIs can take measures to move beyond focusing merely on the entities and individuals on sanctions lists. This effort should start with Know Your Customer (KYC) processes.

1. The institution should consider reviewing its Know Your Customer processes.

FIs will need to adapt their Know Your Customer (KYC) processes to include factors relevant to proliferation financing activity. Understanding whether clients are doing business with proliferating states is essential. If FIs understand the nature of a client's business and the clients and jurisdictions with whom they usually trade, it will become easier to mitigate for any potential risk of proliferation financing activity. As the Chinpo Shipping Company case study demonstrates, had the financial institution in question devoted time towards a more extensive KYC effort, it would have quickly discovered that 100% of the client's business was connected directly to North Korea.

Having a greater awareness of exposed clients will help FIs to understand the extent of the risk they are facing. Most institutions already ask new clients about their usual trade patterns and suppliers/buyers lists. Should any future transactions deviate from this activity, this can more easily be flagged because institutions have a well-developed understanding of what constitutes 'normal'.

However, RUSI has found that many FIs do not include questions relevant to proliferation financing in their due diligence process – whether at the on-boarding stage or over the course of the client relationship.[2] It is also true that trade finance operations within FIs often work separately from wider compliance functions. Compliance staff may therefore not have the information they need to adequately monitor clients who could otherwise be determined as high risk for proliferation finance activities. Similarly, financial institutions should also take steps to ensure that the due diligence procedures of their clients, particularly those involved in the manufacturing and trade of sensitive items, is comprehensive, ensuring the client has a clear idea of who they are trading with and the potential end-use of their products.There are a number of questions FIs should address to upgrade their KYC processes as it relates to proliferation financing risk. For example:

- Does your institution consider proliferation financing threats in the on-boarding process of new clients?
- Do you ask potential new clients whether they have ever had trade relationships with proliferating jurisdictions?
- Is your institution regularly updating its client due diligence records, particular the records of clients with frequent China- or Southeast Asia-based business.

2. Dall et al., 'Out of Sight, Out of Mind?', p. 22.

- If companies trading with proliferating states, such as North Korea, are within your risk appetite, do you currently subject those accounts to enhanced due diligence? Do you flag any bulk cash withdrawals from the account?

2. Investigating known proliferation networks for a possible connection to the institution.

FIs may choose to move further beyond a list-based approach, by dedicating resources to studying previous proliferation finance cases to gain a better understanding of the wider network of actors involved in proliferation financing activities. As previously mentioned, UN panels monitor countries' implementation of sanctions obligations and also provide detailed information on recent illicit activities and evasive practices. For example, the Panel established pursuant to UNSCR 1874 provides detailed information on North Korea's procurement and related proliferation financing activities, and includes the names of entities and individuals involved in these activities. Some of these entities and individuals may not have been sanctioned formally by the UN, but still maintain a significant involvement in procurement and proliferation financing activities. There are also a number of non-governmental sources that can be consulted for advice on proliferators' evasive patterns, including detailed case studies on proliferators' use of the formal financial system. A list of relevant sources can be found in Annex 1.

Investigating the wider networks of designated entities can reveal links that are not otherwise immediately obvious. Some FIs have had success using such reports as a starting point for moving beyond an approach to CPF which relies on list-based screening. They may also gain a better understanding of what trends to look out for in terms of CPF activity where no immediate connection to designated entities is apparent.

Sanctions lists as well as UN Panel of Experts reports contain names of entities and individuals involved in proliferation activities, but also other identifying information, including addresses, names of directors, email addresses and phone numbers. FIs can check whether any of their clients share any of these same contact details, and if so, conduct further analysis into how they are connected to the wider proliferation network.

3. Investigating specific clients or past cases for links to proliferation networks.

FIs, depending on their own determination of exposure to proliferation financing risk, may choose to single out specific clients or cases for further investigation. FIs can consult open-source databases, such as company registries to gain more information into shareholders and directors of clients, and determine whether any of these individuals are either designated on international sanctions lists, or connected to other entities and individuals who are.

Identifying Proliferation-Sensitive Goods and Technology

Because proliferation financing activity is sometimes connected to an underlying movement of goods, some argue that FIs may benefit from screening documentation received in support of financial transactions in search of dual-use or controlled goods. Such goods may be specific components and technologies, as well as raw materials and software systems. Goods which are considered controlled or sensitive in terms of their potential end-use applications are monitored and listed in international export control regimes (See Box 3).

Box 3: List of Relevant Export Control Regimes and Their Areas of Focus.

- Nuclear Suppliers Group. Nuclear materials and technology needed for nuclear programmes, as well as technology which is considered dual-use and may be used in nuclear programmes.
- Missile Technology Control Regime (MTCR). Focuses on technology needed for developing WMD delivery systems.
- Wassenaar Arrangement. Limited to conventional arms trade controls, as well as specific dual-use goods which may be applicable to illicit proliferation programmes.
- The Australia Group. Focuses on materials and technology needed for chemical and biological weapons development.
- Zangger Committee. Includes a list of technology needed for the production of fissile nuclear material.

The European Union maintains a list of dual-use and controlled items, which incorporates the above export control regimes, in Council Regulation No 428/2009 and its subsequent amendments.

The need to screen for dual-use or controlled goods is an obligation promoted by certain governments, namely the US and the UK, and many financial institutions in these jurisdictions have therefore made steps to screen for proliferation-sensitive goods and technology within their trade finance business. There are however certain challenges in doing so, as outlined in Box 4.

These expectations are not always communicated in other jurisdictions, and there is a debate both between governments and within FIs over the merits of screening documentation received in support of financial transactions in search of dual-use or controlled goods (See Box 4). It should again be noted that proliferation financing also extends into activities not directly connected to the physical movement of goods.

While many FIs do not feel they have the technical expertise among their staff to fully incorporate lists of goods into their internal compliance processes, some have embarked on efforts to screen against goods and technology. This is a difficult exercise, mostly because very few details are provided in payment instructions regarding goods and technology being shipped. In cases where the transaction is backed up by trade documentation (for example in a letter of credit), the information supplied to the FI would, in many cases, not be specific enough to determine its

potential end-use. Certain FIs have instead chosen to categorise dual-use items by the export control code they would fall under, either using Harmonized Tariff Schedule codes or European control codes. In many cases, however, a specific export control code will not give a conclusive indication that a product is controlled, and a subsequent (and often detailed) investigation is therefore required.

Box 4: Excerpt From 'Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance'.

Those who suggest [screening for proliferation sensitive goods] is neither the job of FIs, nor realistically within their capabilities, present several supporting arguments. First, those checking the documentation a bank receive in support of a trade finance product application do not have the technical expertise required to determine whether a good meets control thresholds…

Second, even if banks did have this expertise, the documentation provided often does not contain sufficient technical detail to make a decision about the potential need for an export licence…

The third argument advanced is therefore that it should be the role of customs authorities, freight forwarders or shipping companies to make determinations about the potential dual-use nature of the goods in question. Finally, they note that proliferators and other illicit actors engaging in trade are adept at forging and falsifying documentation to conceal a range of information, including the nature of goods. North Korea, for example, is known to have a penchant for identifying military-related goods it sells overseas (including missile-related products) as 'spare parts' for construction machinery...

By contrast, those who contend that screening for dual-use goods … maintain that it is possible to screen for 'obvious' dual-use goods, even though what constitutes 'obvious' will inevitably be a subjective assessment. Finally, they note that document falsification is in some proliferation-related scenarios actually highly unlikely. Proliferating countries such as North Korea still seek dual-use goods from reputable suppliers overseas, often declaring false end-users in order to dupe suppliers into exporting those products. In these cases, the reputable seller would in all likelihood fill in trade documentation correctly.

Source: Dall et al., 'Out of Sight, Out of Mind?', p. 24.

FIs should consider both arguments and carefully consider whether they are exposed to potential trade in illicit goods to an extent that warrants efforts to screen against goods and technology in financial transactions. Furthermore, while efforts to screen specifically for proliferation-sensitive goods and technology may be difficult, FIs can also enhance their efforts in this space by a method of exclusion. For example, rather than integrating export control lists into screening software (an effort which may have limited results), FIs can take steps to identify which clients are of less risk to trading in sensitive goods and technologies or jurisdictions which are less exposed, and concentrate efforts on those that remain.

FIs may also wish to focus their efforts on a list of items currently being sought by a specific proliferating state, and UN reports which detail procurement attempts by North Korea are therefore useful in detailing the type of items and technology they currently desire.

1. Institutions should consider the extent of their general trade business.

As proliferation financing occurs in support of an underlying movement of goods, extensive trade business operations could be more exposed to proliferation financing activity. If FIs have general trade finance business they should therefore consider whether sufficient measures are in place to ensure that this arm of the business is not exposed to proliferation finance activity. For example:

- Does your institution have significant trade business in Singapore (or other exposed jurisdictions)?
- When facilitating trade finance business, does your institution conduct further analysis into the goods being shipped?
- How integrated are trade finance operations in the compliance procedures of the institution?

Based on the answers to these questions, an FI can determine whether further measures, some of which are outlined below, are needed to mitigate its exposure to proliferation financing risks. In doing so, FIs should factor in the various obligations at the international and national levels with which they are expected to comply – whether formally written into law or informally communicated by individual governments.

Available on the website of the Nuclear Suppliers Group, is a set of 'good practices' authored by the UK government to help companies, including those in the financial sector, that helps reduce the risk of supporting illicit procurement activities for WMD programmes. The good practices, while not legally binding, include:

- Implementing 'internal systems to ensure due-diligence checks are carried out on potential customers and business partners and the goods … utilising public information such as early warning lists, red-flag checklists and questionnaires provided by the United Nations, States and other parties'.
- 'Consult government export control authorities before having any dealings with entities identified as being of proliferation concern either from public sources, from corporate monitoring systems or from contact with relevant competent authorities'. This recommendation would be seen to incorporate both those entities identified on sanctions lists, as well as those not-yet-designated but with a connection to a relevant jurisdiction of proliferation concern.
- 'Foster an open and transparent relationship with appropriate government and regulatory authorities'.[3]

3. The full document can be accessed at: <http://www.nuclearsuppliersgroup.org/images/Files/National_Practices/NSG_Measures_for_industry_update_revised_v3.0.pdf>.

2. The institution should determine whether any of its clients are involved in the sale of sensitive WMD technologies.

FIs may also choose to implement a goods-based approach to CPF by focusing on the trade activities of their customers, rather than the goods themselves. FIs can begin this effort by developing a general understanding of procurement patterns and determine whether any of its clients could be involved in the sale of sensitive WMD technologies. This is where KYC processes which include information relevant to proliferation financing risk will be helpful for FIs in gaining a better understanding of their clients and their operations.

It should be noted however, that while businesses may not be involved in the direct sale, manufacture or transporting of WMD technology, they may still be exposed as facilitators, middlemen or in other areas of illicit trade in support of WMD programmes.

If financial institutions devote greater attention to companies who are involved in the supply chain of WMD and related delivery technology, 'those clients would be more likely to improve their compliance and risk management' in return.[4] This should, however, not preclude wider efforts to mitigate against the proliferation financing risk stemming from the procurement of goods below control thresholds. For example:

- Has your institution identified clients who either manufacture or trade in sensitive goods and technology? If so, these clients may be targeted by proliferators and your FI should consider putting in place enhanced due diligence measures on these transactions.
- If any of your clients trade in sensitive items, is your FI familiar with the client's trading partners and regular trading patterns? Does your client ship goods to individuals or companies located in jurisdictions which are known to host extensive corporate networks operated by proliferators (for example China, Singapore, Malaysia, Hong Kong for North Korea)? While these goods may be for legitimate end uses in these jurisdictions, your FI should also be aware of the potential for goods to be transshipped on to a proliferating country.
- Does your national government provide a registry of companies involved in the export of controlled items and other sensitive trade activities? Do you have clients on this list?

4. Rachel A Weise and Gretchen E Hund, 'Financial Incentives for Reducing Proliferation Risks', *Bulletin of the Atomic Scientists* (Vol. 72, No. 5, August 2016), p. 335.

Key Points:

- Proliferation finance may share certain characteristics with other forms of financial crime, but it should be countered as a financial crime risk in its own right.
- Unlike other financial crime risks, such as money laundering and terrorist financing, of which FIs have greater experience and knowledge, proliferation finance tends to be directed by state actors, such as North Korea and Iran.
- Financial institutions should carry out an internal risk assessment to determine their exposure to proliferation finance, and to better understand what measures should be put in place to mitigate the risk. This will include answering a number of questions regarding its client base, correspondent banking relationships, current due diligence measures, the extent of its trade finance business and its activities in jurisdictions where proliferators are known to maintain large corporate networks.
- Financial institutions should take measures to move beyond focusing merely on the entities and individuals on sanctions lists. This includes conducting network analysis in order to determine whether any clients are connected to or doing business with designated entities.
- Institutions may consult proliferation finance case studies to gain a better understanding of evasive patterns and techniques employed by proliferators. Specifically, financial institutions should consult reports by the UN Panel of Experts.
- Financial institutions should familiarise themselves with export control lists as well as be aware of any clients who are either sellers or manufacturers of proliferation-sensitive goods and technology, and who may be targeted by proliferators. Your institution should monitor the end use of these products, rather than the products themselves in these cases.
- Financial institutions should consult lists of indicators and red flags of proliferation finance, but be aware of the limitations of these lists.

Conclusion

FINANCIAL INSTITUTIONS HAVE a role to play in preventing proliferators from accessing the formal financial system and providing financial services in support of proliferation-sensitive trade. Still, financial institutions suffer from a lack in their capability to detect and disrupt proliferation finance activities, due to varying government initiatives and mixed messages passed down from governments and regulators to the financial sector.

It is important that financial institutions take time to better understand and mitigate proliferation financing risk. Proliferators have become increasingly skilled in circumventing the sanctions put against them, and gain access to the financial system through extensive networks of corporate entities (including front companies), middlemen and circuitous payment patterns. In most cases, there will be no obvious paper connection to jurisdictions of proliferation concern.

For financial institutions that have carried out little or no concerted thinking on this subject as distinct from other forms of financial crime, there is however a number of approaches which can easily be adopted to better mitigate the institution against proliferation financing risk. The first step is education about the risk at hand. This includes conducting an internal risk assessment to better understand potential exposure to proliferation financing and the areas of concern which would require mitigation. Financial institutions should also undertake efforts to move beyond focusing merely on the entities and individuals listed on sanctions lists, and instead familiarise themselves with the wider networks of proliferating actors.

While no approach to countering proliferation finance is fool-proof, a few simple adjustments to internal policies can go a long way to ensuring that a financial institution has a baseline policy for dealing with proliferation financing risk, and can help mitigate the risk of inadvertently being caught up in proliferation financing activity.

Adopting these measures will secure the financial institution against unnecessary risk, as well as contributing towards an important international security objective of preventing the further spread of WMD capabilities, and obstructing the efforts of proliferators to obtaining the technologies and tools needed to develop such capabilities.

Emil Dall *is a Research Fellow in the Proliferation and Nuclear Policy Programme at RUSI.*

Tom Keatinge *is the Director of the Centre for Financial Crime and Security Studies (CFCS) at RUSI.*

Andrea Berger *is an Associate Fellow at RUSI and a Senior Research Associate and Senior Program Manager at the James Martin Center for Nonproliferation Studies.*

Annex 1: List of Relevant Sources for Case Studies of Proliferation Networks and Activity

International Organisations:

- Annual Reports by the United Nations Panel of Experts established pursuant to resolution 1874 (North Korea). https://www.un.org/sc/suborg/en/sanctions/1718/panel_experts/reports
- Financial Action Task Force Typologies Report on Proliferation Financing, 18 June 2008. http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

Non-Governmental Sources:

- Project Alpha, Centre for Science and Security Studies at King's College London. Comprehensive database of open-source proliferation finance case studies. www.projectalpha.eu
- James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies at Monterey. Conducts research into non-proliferation and export controls. www.nonproliferation.org
- 38 North, US-Korea Institute at the School of Advanced International Studies. Monitors nuclear and missile developments in North Korea through open-source materials. www.38north.org
- Stockholm International Peace Research Institute (SIPRI). Academic research on dual-use and export control policies. www.sipri.org

Annex 2: Indicators and Red flags of Proliferation Financing Activity

The following table lists the indicators of proliferation finance as supplied by FATF. The second column provides further explanation of these indicators or details a similar indicator from a second source where that helps to clarify the indicator in question.

As mentioned earlier in this report, these indicators are meant to provide FIs with a toolkit to better identify potentially suspicious transactions, although they vary in their degree of usefulness and specificity. During its review of available indicators and guidance on identifying proliferation financing activity, RUSI found that a number of issues should be kept in mind by FIs before they implement these indicators into their internal practices (see page 18). Not all indicators will be feasible for some FIs to carry out and it will be up to individual institutions to determine which indicators are helpful to them, considering the unique risk profile of the institution.

It should also be noted that the appearance of a red flag does not automatically make a transaction suspicious, although they may help to make a determination as to whether further investigation is warranted. It remains the case that the most effective way to mitigate against proliferation financing activity is to develop a sound understanding of the nature of the risk, and adopt internal policies which seek to incorporate an awareness of proliferation financing activity into the everyday compliance procedures of the institution.

	Consolidated list of FATF Indicators	Other sources / Further explanation
Geography/Jurisdiction	Transaction involves foreign country of proliferation concern.	North Korea and Iran are currently top of the list as it relates to countries of proliferation concern. However, other countries and actors may also seek components for WMD and related delivery systems (for example Syria). Similarly, North Korea has been known to supply conventional arms to other parties, in particular Syria, Egypt, the UAE, Yemen and Iran.
	Transaction involves foreign country of diversion concern.	China and certain Southeast Asian jurisdictions are known to host extensive North Korean corporate networks directed by Pyongyang. In China these companies are especially active in Liaoning and Jilin province.
	Trade finance transaction shipment route through jurisdiction with weak export control laws or enforcement.	FFIEC: "Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries" Financial institutions may consult the list of "high risk" and "non-cooperative" jurisdictions issued by FATF: http://www.fatf-gafi.org/countries/#high-risk
	Transaction involves entities located in jurisdiction with weak export control laws or enforcement.	As above.
	Transaction involves shipment of goods inconsistent with normal geographic trade patterns.	Financial institutions should raise questions with their client if goods are shipped through several jurisdictions for no apparent reason (ie. Does not make economic sense).
	Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped. Wolfsberg Group: "Improbable goods, origins, quantities, destination"	While it is difficult for financial institutions to adequately determine the technical capabilities of all countries, a determination can be made by establishing whether receiving countries have industries or sectors involved in (legal) nuclear or missile-related manufacturing or trade.
	Transaction involves FI with known deficiencies in AML/CFT controls or located in weak export control and enforcement jurisdiction.	It is generally believed that North Korea has used correspondent accounts held with Chinese banks to facilitate its international financial transfers.

	Consolidated list of FATF Indicators	Other sources / Further explanation
Trade Documentation	Based on the documentation obtained in the transaction, the declared value of shipment was obviously under-valued vis-à-vis shipment cost.	FCA: "The shipment does not make economic sense" While compliance staff in financial institutions will find it difficult to make a determination whether a specific good is under or over-valued, care should be exercised where it is obvious that the transaction makes little financial sense, either for the seller or the buyer.
	Inconsistencies between information contained in trade documents and financial flows (names, addresses, destinations).	Wolfsberg Group: Covers discrepancies in documents, for example: "Goods descriptions differ significantly" between invoicing and shipping documents, or involves unexplained third parties FCA: "Signifiant discrepancies appear between the descriptions of the goods on the bill of lading and the actual goods" and "changes in shipment locations … or changes in the quality of the goods shipped"
	Freight forwarding company listed as final destination.	N/A
	N/A	FCA: Obvious alterations to third-party documents, eg. customs forms as well as "unusual codes, markings or stamps" BAFT: "Trade-related documentation … appears illogical, altered, fraudulent or certain documentation is absent that would be expected given the nature of the transaction"

	Consolidated list of FATF Indicators	Other sources / Further explanation
Customer	Customer activity does not match business profile or end-user information does not match end-user's business profile.	Wolfsberg Group: The transaction is "beyond capacity or substance of customer" and "totally out of line with customer's known business" FCA: "The customer wishes to engage in transactions that lack business sense of apparent investment strategy, or are inconsistent with the customer's stated business strategy" or their "historical pattern of trade activity" Financial institutions will need to understand the nature of a client's business and the clients and jurisdictions with whom they usually trade . The institution should also have an awareness of which of its clients trade in sensitive goods and technology and be aware of deviations in normal trading patterns of those clients.
	Order for goods placed by firms/individuals from foreign countries other than the country of the stated end-user.	N/A
	Customer vague/incomplete on information it provides, resistant to providing additional information when queried.	FCA: Indicators include customer acting excessively/aggressively or is "reluctant to provide clear answers to routine financial, commercial, technical, or other questions"
	New customer requests letter of credit awaiting approval of new account.	N/A
	The customer or counter-party or its address is similar to one of the parties found on publicly available lists of 'denied persons' or has a history of export control contraventions.	Financial institutions should consult international sanctions lists related to proliferation activities. However, financial institutions should also maintain a list of entities and persons not yet designated, but who are known to have connections to proliferation activities.

	Consolidated list of FATF Indicators	Other sources / Further explanation
Transaction	Transaction demonstrates links between representatives of companies exchanging goods (same owner or management).	FCA: "Transacting businesses share the same address, provide only a registered agent's address, or have other address inconsistencies" BAFT: "Transacting parties appear to … conduct business out of a residential address, or provide only a registered agent's address" In addition to transactions involving connected parties, financial institutions should also be wary of any transacting parties who share addresses or other identifying information with designated entities or entities known to be involved in proliferation activities.
	Transaction involves possible shell companies.	N/A
	Wire transfer/payment from or due to parties not identified on the original letter of credit or other information.	FCA: "Transaction involves an unusual intermediary or number of intermediaries" or "payment is to be made to beneficiary's account held in another country other than the beneficiary's stated location" FFIEC: A customer requests payment of proceeds to an unrelated third party
	Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.	Wolfsberg Group: Payment instructions are "illogical", contain "last minute changes"or there is an "unusual complexity and or unconventional use of financial products"
	Circuitous route of shipment and/or circuitous route of financial transaction.	BAFT: "Transaction structure and/or shipment terms appear unnecessarily complex or unusual and designed to obscure the true nature of the transaction" FCA: "The transaction is an offshore shipment" (the transaction happens in Country A, for a shipment between Country B and C).

Table sources: FATF, 'Typologies Report on Proliferation Financing', June 2008; Wolfberg Group: 'The Wolfsberg Group, ICC and BAFT Trade Finance Principles', Wolfberg Group 2017, <http://www.wolfsberg-principles.com/pdf/home/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf>; FFIEC: Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Infobase, 'Bank Secrecy Act Anti-Money Laundering Examination Manual', <http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_106.htm>; FCA: Financial Conduct Authority, 'Banks' Control of Financial Crime Risks in Trade Finance', Thematic Review, TR13/3, July 2013; BAFT: BAFT, 'Guidance for Identifying Potentially Suspicious Activity in Letters of Credit and Documentary Collections', March 2015.

Annex 3: List of Relevant Financial Obligations Relating to Proliferation Finance in UN Security Council Resolutions

	UNSCR Operative Paragraph	Requirement
Designated Entities, Individuals and Assets	UNSCR 1540, OPs 2 and 3(d)	Criminalises proliferation financing.
	UNSCR 2270, OP 11 (UNSCR 1718 OP 8(d)) UNSCR 2231, Annex B para 6(c) and 6(d)	Targeted financial sanctions (UN designations).
	UNSCR 2270, OP 15	Designated entities' offices to be closed and prohibition on participating in joint ventures and business arrangements.
	UNSCR 2270, OP 32	Targeted financial sanctions (designations of North Korean state entities).
	UNSCR 2270, OP 12	Clarifies that 'economic resources' includes vessels. Also clarifies that economic resources includes 'actual or potential' assets.
	UNSCR 2270, OP 23 UNSCR 2321, OP 12	Freeze vessels.
Proliferation Finance Activity	UNSCR 2270, OP 6 (UNSCR 1718, OP 8(a) and (c))	Prohibit financial transactions to/from North Korea related to the provision, manufacture, maintenance or use of WMD, all arms and related materiel (including 'catch-all' provisions, which enable action to be taken against non-listed items).
	UNSCR 2270, OPs 33, 34, 35 UNSCR 2321, OP 31	Range of prohibitions on FIs (North Korean banks cannot operate branches, subsidiaries etc. abroad, FIs cannot have joint ventures or correspondent banking relationships, FIs cannot open branches, accounts etc. in North Korea).
	UNSCR 2321, OP 16	States must limit the number of bank accounts of North Korean diplomatic missions and consular offices and North Korean diplomats and consular officers.
	UNSCR 2270, OP 36 UNSCR 2321, OP 32	Prohibition on financial support for trade with North Korea.

	UNSCR Operative Paragraph	Requirement
Proliferation Finance Activity (cont.)	UNSCR 2270, OP 37 UNSCR 2094, OPs 11 and 14	Prohibits transfer of bulk cash and gold to North Korea.
	UNSCR 2270, OP 29	Prohibition on supply, sale, transfer of coal, iron and iron ore, with exceptions.
	UNSCR 2270, OP 30	Prohibition on supply, sale, transfer of gold, titanium ore etc.
	UNSCR 2270, OP 31	Prohibition on sale or supply of aviation fuel and kerosene-type rocket fuel, with exceptions.
	UNSCR 2270, OP 19 UNSCR 2321, OP 8	Prohibition on leasing or chartering vessels, aircraft, crew services to North Korea, designated entities, other North Korean entities and entities a State determines has assisted in evading sanctions.
	UNSCR 2321, OP 23	Prohibition on procuring vessels and crew services from North Korea.
	UNSCR 2270, OP 20 UNSCR 2321, OP 9	Prohibition on owning, leasing, operating, providing classification or certification to or insuring a North Korean flagged vessel. Prohibition on registering a vessel in North Korea or seeking authorisation to use the North Korean flag in relation to a vessel.
	UNSCR 2321, OP 22	Prohibition on providing insurance or reinsurance to vessels owned, controlled or operated by North Korea.
	UNSCR 2231, Annex B, Para 2 and Para 4	Prohibition on commercial activities related to Iran without Security Council approval.
	UNSCR 2231, Annex B, Para 2, Para 4 and Para 5	Prohibition on making assets or financial services available or conducting financial transactions related to certain nuclear-related items, ballistic-missile related items and arms and other materiel without Security Council approval, as it relates to Iran.

The authors would like to thank Anagha Joshi for compiling this table.