STATEMENT OF

DR. TOGZHAN KASSENOVA

Senior Fellow
Project on International Commerce, Security, and Economic Statecraft (PISCES)
Center for Policy Research, University at Albany, SUNY

Before the Subcommittee on National Security, International Development, and Monetary Policy for a hearing entitled "The Traffickers' Roadmap: How Bad Actors Exploit Financial Systems to Facilitate the Illicit Trade in People, Animals, Drugs, and Weapons."

THE EXPLOITATION OF THE GLOBAL FINANCIAL SYSTEM FOR WEAPONS OF MASS DESTRUCTION (WMD) PROLIFERATION

Presented
March 4, 2020

The exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation

Dr. Togzhan Kassenova[1]

1. WMD Proliferation as a Security Risk
2. How Proliferation Networks Operate
3. Challenges and Opportunities for Financial Institutions
4. Similarities and Differences with Money Laundering and Terrorist Financing
5. The Role of Public-Private Partnerships

1. WMD Proliferation as a Security Risk

Weapons of mass destruction – nuclear, biological, and chemical weapons - present a persistent risk to the U.S. and international security. If a 10-kiloton nuclear bomb, like the one tested by North Korea in 2013, is dropped in Washington, DC, a fireball of almost 500 feet in radius will cover the city. The radiation will reach such high levels within a half a mile radius that 50-90% percent of people could die without medical help – some of them within hours.[2]

When it comes to preventing WMD proliferation, we need to be conscious of both state and non-state actors. North Korea continues to procure sensitive goods for its nuclear and missile program in defiance of sanctions. Iran is procuring missile-related goods. Agents working on behalf of Syria have sought chemical goods on the commercial market. Several groups, such as Al Qaeda and ISIS, demonstrated interest in acquiring a WMD capability. We do not have a full picture of who might be interested in obtaining a WMD capability in the future.

[1] This testimony is based in part on research findings published in Togzhan Kassenova, "Proliferation Financing: What Financial Institutions Should Know and What They Can Do," ACAMS Today, September-November 2019, pp. 18-22; Togzhan Kassenova, "Challenges With Implementing Proliferation Financing Controls: How Export Controls Can Help," *World ECR: The Journal of Export Controls and Sanctions*, May 2018.
[2] Projection from Alex Wellestein, "Nukemap."

2. How Proliferation Networks Operate

Stealing or buying a ready-made weapon is a next to impossible feat. The main path to a WMD is to procure components, material, and technology and then build a weapon. Because most goods usable in a WMD program are dual-use in nature, with indispensable civilian purposes, they are available on the international commercial market.

The international community attempts to minimize the risk that trade in dual-use and military goods entails. The international export control regimes and national export control systems are designed to regulate trade in sensitive items by requiring traders to obtain licenses. Additionally, the international and unilateral sanctions regimes target known proliferators.

The goal of proliferators and their agents is to acquire goods that can contribute to WMD programs without being caught. Proliferators and their networks continue to defy both export controls and sanctions.

Proliferation networks come in all sizes and shapes. They can be small or large, loose, or more organized. Those buying WMD-related goods can be directly connected to proliferator states, or they can do it purely for profit by inserting themselves into the illicit market to make money.

Proliferators have perfected methods that help them stay under the radar.[3] One of the standard techniques they use is to buy goods that are slightly below the controlled threshold. This means that unless exporting companies are incredibly vigilant,[4] they would not apply for an export license

[3] Daniel Salisbury, "Why Do Entities Get Involved in Proliferation? Exploring the Criminology of Illicit WMD-Related Trade," *The Nonproliferation Review*, 24:3, 2017, 297-314; Daniel Salisbury, "An Evolving State of Play? Exploring Competitive Advantages of State Assets in Proliferation Networks," *Defense & Security Analysis*, January 17, 2019; Daniel Salisbury, "Exploring the Use of 'Third Countries' in Proliferation Networks: The Case of Malaysia," European Journal of International Security, 4:1, 2019,101-122; Glenn Anderson, "Points of Deception: Exploring How Proliferators Evade Controls to Obtain Dual-Use Goods," Strategic Trade Review, Volume 2, Issue 2, 2011, 4-24.

[4] Under "catch-all" provisions of export control systems, companies must apply for a license even for a non-listed item, if there is belief, knowledge or suspicion that good in question may be used in a WMD program.

and subject transaction to government scrutiny. However, these slightly inferior goods can still be used for nefarious purposes.

There is another method proliferators use to avoid government oversight and licensing—they pretend they are ordering goods for a domestic company. In such cases, supplier companies do not have to apply for licenses.

To avoid export controls and sanctions, proliferators lie about the end-use and end-user and hide behind front and shell companies all the time. They never declare that they are buying components for North Korea's nuclear program, Iran's missile program, or Syria's chemical arsenal. For example, they can tell a supplying company they need goods for scientific research or other peaceful purposes. In 2006, an Iranian company ordered sensitive bioresearch equipment from Norway purportedly for a scientific laboratory. On closer look, an attentive Norwegian supplier determined that the equipment Iranians sought was technically superior to what would be necessary for a civilian lab and that it did not fit the physical layout of the laboratory.[5]

Increasingly, shipping companies and vessels are used prominently in sanction evasion. For example, Iran and North Korea falsify documents, reflag vessels, and switch off automatic identification systems to avoid being discovered in the process of illicit transfers of goods.[6]

Supplier companies that provide goods to proliferators can be complicit or not complicit. Larger companies have resources to implement strong internal compliance programs that help them detect any suspicious orders. But some companies, especially smaller ones, do not have resources to invest in compliance and remain negligent. In some cases, supplier companies or individuals within know precisely what they are doing. They do it either because of ideology (to support a sanctioned state) or for profit. In one notorious case, a U.S.-based company MKS Instruments sent pressure transducers to its subsidiary in China after duly applying for a U.S. export license, thinking that the goods would be used in China. The co-opted employee of the MKS Instruments'

[5] For this case and other known cases of proliferation financing, see Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation," Project Alpha, King's College London, October 13, 2017, p 85.
[6] "FinCEN Issues Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System," *Financial Crimes Enforcement Network*, October 11, 2018; U.N. North Korea Panel of Experts report, March 2019, p. 5. The formal name is the Panel of Experts established pursuant to resolution 1874 (2009). For a summary of the report's findings relevant to the financial sector, see Togzhan Kassenova, "2019 U.N. North Korea Panel of Experts Report: Takeaways for Financial Institutions," *ACAMS Today*, March 27, 2019.

subsidiary ordered transducers from an unsuspecting parent company and pretended they would be used by Chinese companies but planned all along to ship those goods to Iran.[7] Pressure transducers can be used in uranium enrichment centrifuges, making possible the production of fissile material that can also be used in a nuclear weapon.

Proliferators prefer to buy good quality goods – mostly from the U.S., European, and Asian suppliers. This means that in most cases, they have to pay for those goods through the formal financial system, making financial institutions part of their proliferation schemes.

3. Challenges and Opportunities for Financial Institutions

Proliferators use formal financial institutions for two main purposes: (1) to pay for procurement of WMD-related goods; (2) to fundraise, launder and move money associated with proliferation activity (for example, this can apply to money that ends up paying for the WMD activity or to profit generated as a result of supplying proliferator states).

Challenges

Financial institutions struggle with identifying and stopping transactions related to procurement, fundraising, and movement of money for illicit WMD programs. Below is the list of key challenges:

Lack of information and capacity to identify financial transactions related to procurement

Financial institutions see limited or no information on goods for which payments are made. The information can be incomplete or even misleading. For example, in one case involving the purchase of chemical equipment from the United States that ended up in Syria, the wire description simply said: "laboratory spare parts."[8] As discussed above, proliferators often order goods just

[7] "Chinese Man Convicted on Charges of Exporting U.S.-origin Pressure Transducers to Iran," *Iran Watch, Wisconsin Project*, February 9, 2016.
[8] Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation," Project Alpha, King's College London, October 13, 2017, p. 63.

below controlled threshold, which means that there is a movement of goods that do not appear on export control lists but can still contribute to WMD programs. There is a big question mark as to whether information that financial institutions receive (through SWIFT or trade finance documentation) is sufficient to check against lists of controlled goods. Transactions happening under open accounts are especially vulnerable since it is not clear what each individual transaction involves. In general, due to limits in technical expertise, it is unlikely that financial institutions on their own will ever be in a confident and comfortable position to analyze if goods are sensitive.

Lack of information on end-use and end-user

In addition to limited information on the goods involved, financial institutions are constrained by a lack of information on end-use and end-users. Even in trade finance transactions, in which financial institutions receive more information on the parties involved, limitations apply. For example, not all parties can be captured from accompanying documentation, either because their signatures are illegible or because they are not key parties to the transactions.

Limitations of the list-scanning approach to risk management

One of the main tools employed by the financial institutions is scanning against lists of sanctioned and/or suspicious entities and individuals. While indispensable, this method has its limitations. First, such scanning returns a high number of false positives (up to 85%), which means that considerable time and effort is spent on clearing those false alarms. Second, concealment and deceit techniques of sanctioned/designated entities and individuals mean that list-scanning does not catch them. They use front and shell companies and the names of associates or family members. Third, the lists contain names of *known* proliferators and are not useful for preventing new (or newly disguised) proliferators from accessing the financial system.

Beneficial ownership of entities

Another vulnerability lies in the uneven implementation of beneficiary ownership controls internationally. European Union countries require collection of data and transparency when it

comes to who owns companies and trusts. Some other major countries, including the United States, are lagging behind.[9] In 2018, FinCEN issued a Customer Due Diligence (CDD) Rule, which applies to covered financial institutions and requires them to identify and verify the identity of beneficial owners of legal entities at the time of account opening and defined points after that.[10] While useful, this rule has limited application. The United States is among the countries that do not require the disclosure of beneficial ownership information at the time of company formation. Proliferators make extensive use of shell companies and get away with hiding behind non-transparent corporate structures.

Correspondent banking

One of the main vulnerabilities to U.S. institutions comes from correspondent accounts as a result of weak controls in foreign jurisdictions and insufficient information on customers behind transactions originating in respondent banks. WMD proliferation financing networks exploit correspondent banking to move funds through U.S. correspondent accounts.[11]

Absence of proliferation financing risk assessment and dedicated proliferation financing component in "Know-Your-Customer" (KYC) and transaction monitoring procedures beyond sanctions compliance

Preventing proliferation financing requires more than compliance with sanctions since sanctions do not address potential proliferators. For that purpose, national and institutional proliferation financing risk assessments, as well as the integration of proliferation financing components into KYC and transaction procedures, are critical. The United States was among the first to conduct a national proliferation financing risk assessment.[12] However, proliferation financing risk assessments at the level of financial institutions are neither a norm nor a requirement. Similarly,

[9] Nate Sibley, "Countering Chinese Communist Party Threats with Corporate Transparency," Hudson Institute, 2019; "The Library Card Project: The Ease of Forming Anonymous Companies in the United States," Financial Integrity Institute, 2019.
[10] See discussion on beneficial requirements in "National Strategy for Combatting Terrorist and Other Illicit Financing," 2020, pp. 13-15.
[11] See discussion on correspondent banking in "National Strategy for Combatting Terrorist and Other Illicit Financing," 2020, pp. 21-22.
[12] "National Proliferation Financing Risk Assessment," 2018.

KYC and transaction monitoring procedures at financial institutions normally do not include a proliferation financing component that could help identify specific risks that a particular institution faces.

Vulnerabilities in the cyber and crypto domain

North Korea is a poster child for how vulnerabilities in the cyber and crypto domain can be exploited to generate funds for illicit purposes, including for a WMD program. North Korea's intelligence agency —Reconnaissance General Bureau—leads and coordinates cyberattacks to force the transfer of funds from financial institutions and cryptocurrency exchanges. For example, in 2018, the Reconnaissance General Lab group forced the transfer of $10 million from Banco de Chile mainly to accounts in Hong Kong.[13] North Korea targets not only brick-and-mortar financial institutions but cryptocurrency exchanges as well. In 2018, in one attack on a cryptocurrency exchange, North Korean hackers stole close to $250 million in cryptocurrency.[14] North Korean agents launder cryptocurrency (mined, stolen, and received through ransomware) via a complex web of online transactions.[15]

Opportunities

Financial institutions can be critical in the fight against illicit activity related to weapons of mass destruction. Noting limitations in the capacity required to identify proliferation-relevant goods, the financial institutions should focus on a better understanding of customers and patterns in transactions, rather than on trying to understand the technical characteristics of goods. Such an approach will also be helpful in uncovering transactions that are not directly relevant to procurement (i.e., payment for goods) but that can still contribute to proliferation (i.e., fundraising, moving, and laundering funds associated with proliferation activity).

[13] U.N. North Korea Panel of Experts report, March 2019, p. 51.
[14] "2 Chinese Nationals Charged in $100M Cryptocurrency Scheme," The Associated Press, *New York Times*, March 2, 2020.
[15] U.N. North Korea Panel of Experts report, August 2019, pp. 26-30.

Incorporating a proliferation financing component into KYC and transaction monitoring procedures can significantly increase the chances of uncovering "red flags." Below are some recommendations for KYC procedures:

- Including information on the line of business in customer profiles and denoting whether business and/or activities involve dual-use and/or military goods. More detailed information on the type of business and/or activities can be requested from customers as part of service suitability for higher-risk/vulnerable products like trade finance or wires.
- Using data from a broader array of lists in addition to U.S. legally binding lists for scanning. For example, foreign countries, international and nonprofit organizations, and commercial vendors develop lists of parties *suspected* in proliferation for export control compliance purposes.
- Better scrutiny of phone numbers and addresses. It is not uncommon for front and shell companies to share managers, addresses, and phone numbers.

Similarly, there are specific steps that can be integrated into transaction monitoring, including but not limited to:

- Greater automatic scrutiny of transactions involving accounts of the individuals and entities identified as sensitive (these can include individuals that could be associated with sanctioned activities; businesses that trade in dual-use and/or military goods; businesses commonly implicated in proliferation financing-related activities - shipping companies, trading houses, exchange houses, etc.)
- Scanning transactions against a broader array of lists. Incorporating scanning against foreign governments' proliferation-relevant lists can prove especially useful when providing trade finance services.
- Adopting technical solutions to monitoring trade finance transactions that are more sophisticated and efficient than a manual review of trade documents. This can involve, for example, adopting blockchain-based trade finance platforms or harvesting unstructured data (wire data, transaction memos, suspicious activity reports (SARs), negatives news, etc.).

- Incorporation of tailored geographical factors into transaction monitoring such as specific cities and regions that are known to host agents working on behalf of proliferating states. For example, the U.S. "National Proliferation Financing Risk Assessment (NPFRA)" notes that many front companies working on behalf of North Korea are based in the Dalian, Dangdong, Jinzhou, and Shenyang municipalities in the Liaoning province as well as Hong Kong.[16]
- Filing SARs on any transactions that do not make sense, as these might help uncover proliferation networks.
- Inserting a provision in trade finance service contracts to allow an institution to exist a transaction or a relationship without a penalty if the customer does not identify transactions involving sensitive goods or if there are other concerns about a transaction.

4. Similarities and Differences with Money Laundering and Terrorist Financing

Patterns of proliferation financing have both similarities and differences with other types of financial crime, such as money laundering and terrorist financing. Similar to money launderers, proliferators favor formal financial systems because the goods they procure mostly come from legitimate manufacturers. As with money launderers, proliferators rely on shell and front companies to avoid detection. Similar to terrorist financing and unlike money laundering, proliferation financing does not usually involve strikingly large amounts. In another similarity with terrorist financing and unlike money laundering, the money trail is linear – the money is generated to purchase goods.[17] There are two main differences between proliferation financing, on the one hand, and money laundering and terrorist financing. First, transactions related to WMD procurement look like legitimate commercial activity. Second, in addition to individuals, entities, and transactions, there is an emphasis on goods (on which financial institutions do not have expertise).

[16] "National Proliferation Financing Risk Assessment," 2018, p. 18.
[17] Please see Annex 3, "Comparison of ML with TF. and FoP" in Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation," Project Alpha, King's College London, 2017, p. 35.

It is necessary to employ proliferation-specific tools to minimize proliferation financing due to the above-mentioned differences in typologies, but it is also worth approaching various kinds of illicit financing holistically. We know, for example, that proliferators and agents working on behalf of proliferating states engage in other types of financial crime. The most notorious case is North Korea, which exploits the global financial system to fundraise money from various licit and illicit activities, move and launder funds, and pay for its WMD program.[18] In another example involving an individual, a Chinese middleman Karl Lee for years supplied (and likely continues to supply) Iran with missile-related components. He has used the global financial system not only in support of his procurement and trade efforts but also to launder proceeds from such sales.[19]

Even if a financial institution cannot be sure that they are dealing with a proliferation-related case, it is important that they flag/stop a transaction that appears suspicious to them. In some cases, proliferation financing was uncovered by a financial institution because of suspicious indicators related to money laundering.[20] Increasing the capacity to deal with one type of financial crime automatically increases the overall capacity to detect other types of illicit financing.

5. The Role of Public-Private Partnerships

Financing of WMD proliferation is a difficult task that no government agency or financial institution is in a position to confront individually. In that sense, public-private partnerships have great potential. It is not general practice for financial institutions to interact with export control, Customs, or border security agencies. Typically, the interaction between financial institutions and law enforcement/intelligence authorities is one-way through either SARs (on which financial institutions do not receive feedback) or in response to legally mandated requests for disclosure of information.

[18] UN North Korea Panel of Experts report, August 2019, p. 4.
[19] "Li Fangwei in Rem Complaint and S1 Indictment," United States District Court, Southern District of New York, 2014.
[20] Jonathan Brewer, "Study of Typologies of Financing of WMD Proliferation," Project Alpha, King's College London, October 13, 2017, p. 121, 122.

Creating opportunities for all actors involved in combatting WMD proliferation to share information can help uncover proliferation networks, sanctions evasion, and cases of proliferation financing. For example, export control authorities have technical expertise on dual-use and military goods; they also have information on export license approvals and denials, as well as 'black-lists' of violators that can be helpful to financial institutions. Customs and border security agencies have information on the movement of sensitive goods and valuable enforcement data. While financial institutions are constrained when it comes to disclosing proprietary information, timely sharing of observations on trends and patterns of illicit financial movements can prevent proliferation financing from happening, as well as add to our understanding of how proliferation networks operate and finance their activities.

Existing public-private partnerships, such as FinCEN Exchange in the United States, the Joint Money Laundering Intelligence Taskforce (JMLIT) in the United Kingdom, Fintel Alliance in Australia, and others, are a great start. Going forward, it is worth considering how to involve smaller and medium-size banks into such partnerships.

Finally, academic institutions, NGOs, and think-tanks are becoming increasingly indispensable in confronting proliferation financing by contributing to research and capacity-building efforts. They should be recognized as important actors and utilized fully as a valuable resource.