PROLIFERATION FINANCING:

What financial institutions should know and what they can do

Is it possible for a company with no website and no stated business purpose in its corporate documents—acting on behalf of a sanctioned North Korean bank—to use the U.S. financial system? Worryingly, the answer is yes. Mingzheng, a Hong-Kong based company, sent and received wires in U.S. dollars on behalf of a foreign trade bank that was involved in Pyongyang's weapons of mass destruction (WMD) program.[1] In 2017, the U.S. Department of Justice (DOJ) brought a civil asset forfeiture complaint for the $1.9 million associated with Mingzheng. The money was held at six U.S. financial institutions (FIs).[2]

Unlike money laundering and terrorist financing, proliferation financing is a less understood challenge. This article describes WMD proliferation risks and methods used by proliferators and offers some ideas on how FIs can contribute to the fight against the spread of WMD material, components and technology.

Weapons of mass destruction

There are three types of WMD: nuclear, biological and chemical. Nuclear weapons are most devastating in their potential to destroy and kill. If a 10-kiloton nuclear bomb (like the one tested by North Korea in 2013) is dropped in Washington, D.C., a fireball of almost 500 feet in radius will cover the city. The radiation dose will reach such high levels within a half a mile radius that 50-90% of people could die without medical help—some of them within hours.[3]

Nine countries possess nuclear arsenals today; the U.S., Russia, China, France and the United Kingdom (U.K.) are officially recognized as nuclear-weapon states by the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) that was signed in 1968. Most of the other countries signed the NPT as non-nuclear weapon states.[4] The treaty was designed to cap the number of nuclear states at five, but India, Pakistan and Israel never signed it and still went on to develop nuclear weapons. North Korea, formerly a member of the NPT, left in 2003 and developed nuclear weapons. It now has 20-30 nuclear weapons and enough nuclear material to build another 30-60.

There are almost 14,000 nuclear weapons in the world today—enough to kill the entire planet many times over. A single nuclear attack can claim thousands of victims. More than 90% of all nuclear weapons belong to the U.S. and Russia.

Chemical weapons that include nerve agents, blister agents, choking agents and blood agents are banned, but several countries are suspected or confirmed to have chemical warfare programs. The Syrian government now uses chlorine gas against its own citizens. International law also bans biological weapons, but several countries are suspected of carrying out biowarfare research. Chemical and biological weapons cannot kill as many people as nuclear weapons, but they can cause painful injuries and deaths.

Non-state actors, such as terrorist organizations and individuals, can also use WMD, as was the case with cult organization Aum Shinrikyo using sarin gas in Tokyo subways or the anthrax letters sent to U.S. senators.

Stopping proliferation

Today, preventing the spread of WMD is not about how the ready-made weapon gets into proliferators' hands—this remains a next to impossible feat for them. It is about finding ways to stop the illicit acquisition of components and material that can be used to build weapons or missiles used to deliver them.

The challenge is that such components and materials include dual-use goods and technology, which have peaceful and military applications. Economies around the world rely on such goods and technology and companies need to procure them in a timely and efficient manner.

What is a dual-use good? For example, a triggered spark gap (a small unassuming-looking object the shape of a spool) is indispensable in a medical device called lithotripter. This device passes electromagnetic shock waves through a water bath while a patient sits inside, allowing pulverized stones to leave the body naturally. However, a triggered spark that meets specific technical characteristics can also be used to trigger a nuclear device explosion.

Goods and technology that can be used in weapons programs, including dual-use items, are collectively referred to as strategic. How can it be ensured that countries can trade in strategic goods and technology without contributing to proliferation? The answer is export controls.

There are four multilateral export regimes: Australia Group, Nuclear Suppliers Group, Missile Technology Control Regime and the Wassenaar Arrangement. Each deals with a specific category of goods and technology: biological and chemical, nuclear, missiles and conventional weapons. All four regimes regularly update their control lists—lists of items that require extra attention when traded. Countries with advanced export control systems adopt these control lists and require licenses for export, import, transit, transshipment, brokering and other activities involving such goods. What this means in practice is that a company wishing to sell its strategic goods to another company abroad has to go to its government first and request an export license. The government checks if the end use and end user are legitimate and that the product will not end up helping a weapons program—only then will it grant the license.

In turn, the sanctions regime of the United Nations (U.N.) and individual countries are designed to prevent the most notorious proliferators from acquiring goods that could contribute to their WMD and missile programs or generating income that could pay for these programs.

These additional controls on the flow of strategic goods in place made life somewhat harder for proliferators—but they did not give up. Instead, they devised ways to circumvent export controls and sanctions.

How proliferators operate

The goal of proliferators is to acquire goods that can contribute to WMD programs without being caught. Proliferation networks come in all sizes and shapes. They can be small or large, loose or more organized. It can even be just one person with internet access ordering and then retransferring sensitive goods. Those buying strategic 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.[5] 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 extremely vigilant,[6] they would not apply for an export license 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.

Proliferators lie about the end use and end user as well as 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 disguised as 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.[7]

Another especially favored method by North Korea is the use of diplomatic cover in proliferation-relevant procurement and fundraising. The 2019 report from the U.N. North Korea's Panel of Experts documents a persistent trend—North Korean diplomats stationed overseas act as procurement agents for their country's WMD program and use their bank accounts in developing countries to pay for goods.[8] Iran is also known for misusing state institutions to evade a broad range of sanctions. For example, officials from the Central Bank of Iran are known to help illicit networks working on Iran's behalf.[9]

Increasingly, shipping companies and vessels are used prominently in sanctions 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.[10]

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' 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.[11] Pressure transducers can be used in uranium enrichment centrifuges, making possible the production of nuclear fuel that can be used in a nuclear weapon.

Proliferators need to pay for the items they buy, and in most cases—they have to do it through a formal financial system, making FIs part of their proliferation schemes. For financial transactions supporting proliferation activity, they use front and shell companies, agents and brokers, and engage in elaborate schemes that obscure real parties from the transactions.

What can financial institutions do?

The current level of proliferation financing controls around the world is at an early stage, with rare exceptions. By default, the majority of governments and FIs hold a narrow view of what proliferation financing controls mean. For them, sanctions implementation equals curbing proliferation financing. In reality, proliferation risks extend beyond what sanctions cover. Sanctions are by design reactive, punishing and deterring of known proliferators. To be truly effective, proliferation financing controls must cast a wider net designed to catch anyone who attempts to engage in illicit activity.

Even within the narrow task of sanctions implementation, FIs face many challenges. These include a high number of false positives when list scanning against sanctioned parties, inability to identify proliferation-relevant transactions due to lack of information, as well as capacity and deception techniques employed by proliferators.

On a fundamental level, FIs alone cannot prevent or uncover proliferation financing. On the procurement side, the main reason for this is the distance and disconnect between the financial transactions and proliferation-related goods. Supplier companies know their products best, understand how their products can be used and can refuse to supply them to suspicious end users. They are the first line of defense to prevent proliferation. Export and import control licensing authorities are the second line of defense, as they can deny permission for goods to leave or enter the country. Finally, customs and border security officers are the third line of defense. They have access to relevant documentation (licenses, cargo description, bill of landing, etc.) and can physically inspect the goods if necessary. In comparison, FIs see less information about the goods involved and have no technical expertise on goods.[12]

Identifying transactions that are not directly related to the procurement of goods but that can contribute to proliferation—such as fundraising and laundering of funds that could later be used in WMD programs—is even more difficult.

Nevertheless, FIs can and should play an important part in the fight against proliferation.[13] Below are some ideas on relatively easy steps FIs can take to strengthen their capacity to implement proliferation financing controls, including adopting methods and techniques from the export control field.

First line of defense: Integration of a proliferation financing component into KYC

FIs should begin to include a proliferation-specific component in know your customer (KYC) procedures.

First, customer profiles should include the information on the line of business and denote whether business and/or activities involve strategic goods. The government agencies in charge of trade, industry and export controls can provide guidance to the financial sector on relevant companies exporting or importing strategic goods in a given country. More detailed information on the type of business and/or activities can be requested from clients as part of service suitability for higher-risk/vulnerable products like trade finance or wires. In cases when different teams within an FI are responsible for different types of compliance risks, better coordination and information flow as well as a clear allocation of responsibility would help avoid strategic trade-related checks falling through the cracks. For example, corporate compliance teams that may have exposure to export control versus financial crimes teams that may have exposure to anti-money laundering and the Office of Foreign Assets Control.

Second, as part of KYC, FIs should consider using data from a broader array of lists in addition to their home country's legally binding lists. In the U.S., the Bureau of Industry and Security offers lists of parties of concern consisting of the denied persons list, entity list, unverified list and consolidated screening list. In Japan, the Ministry of Economy, Trade, and Industry provides its industry with the "end-user list."[14] Other countries develop their own lists. In addition to governments, international and nonprofit organizations as well as commercial vendors develop lists of parties suspected in proliferation for export control compliance purposes. However, it should be noted that ingesting more lists into scanning software might increase the number of false positives.

Third, even the scrutiny of the physical addresses and phone numbers provided at the time of a customer's onboarding can help uncover early "red flags." For example, it is not uncommon for procurement agents acting on behalf of North Korea to use the same addresses as the embassies/representation offices of North Korea. Also, North Korean front companies often share managers, owners and phone numbers.

Fourth, in response to a well-documented trend of North Korean diplomats and individuals holding North Korean diplomatic passports acting as procurement agents, FIs might consider introducing special procedures for account opening by North Korean citizens. Such procedures can include confirming that North Korean diplomats are accredited to work in a given country, tying the life period of an account to an official period of accreditation in the country and making sure that North Korean

diplomats do not open multiple accounts in the names of their associates or front companies.[15]

Second line of defense: Transaction monitoring

Transaction monitoring should also integrate a proliferation financing component. First, transactions involving accounts of the individuals and entities identified as sensitive should automatically receive greater ongoing scrutiny. For example, North Korean diplomats; individuals that could be associated with sanctioned activities; businesses that trade in strategic goods or that are commonly implicated in proliferation financing activities such as shipping companies, trading houses, exchanges houses, etc.

Second, similar to running checks against proliferation-relevant lists as part of the customer onboarding stage, it would be prudent to scan the names of all parties to transactions against such lists as part of transaction monitoring. Incorporating scanning against foreign governments' proliferation-relevant lists can prove especially prudent when providing trade finance services since trade transactions cross multiple borders.

Third, more comprehensive customer profiles created at the time of onboarding that identify customers who trade in strategic goods will help with risk management. FIs can identify regular patterns in strategic trade transactions that do not require extra scrutiny and at the same time stay vigilant of new or unusual transactions by such customers. Similarly, having a clear idea of customers' line of business will alert FIs to transactions that do not correspond (e.g., a company that does not have anything to do with strategic goods suddenly starts carrying out transactions involving them).

Fourth, FIs should adopt more adequate controls to monitor transactions that involve strategic goods. Now transaction monitoring for trade finance includes a manual review of all paper documents and screening parties to the transaction against a chosen solution (list-scanning software). However, not all parties can be captured in the process, either because their signatures are illegible or because they are not key parties to the transactions. Manual reviews of trade documents to identify parties and goods involved do not seem adequate for identifying proliferation activity.

A couple of emerging technical solutions might prove helpful in this regard. HSBC's pilot blockchain-based trade finance platform Voltron is designed to increase transparency and reduce transaction time.[16] While a reduction of transaction time is likely the primary commercial motivation for such a platform, increased transparency on all parties across the supply chain will help an FI have a better understanding on parties and goods involved.

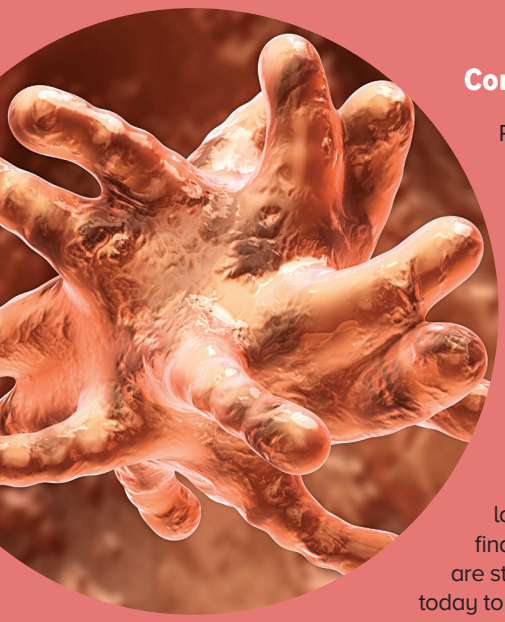
Another innovative approach that can be relevant involves harvesting unstructured data, such as wire data, transaction memos, case data, suspicious activity reports (SARs), negative news, texts of email/phone/chat conversations, law enforcement requests and trade documents. Proponents of this approach point out that such tools can help with new insights and patterns into a potentially illicit activity that does not manifest in traditional structured data.[17]

Fifth, geographic factors should be included in transaction monitoring systems. For example, the U.S.' National Proliferation Financing Risk Assessment (NPFRA) notes that many North Korean front companies are based in China or use Chinese banks. While putting an alert for an entire country (in this case, China) might not be efficient, FIs might consider subjecting to extra scrutiny transactions involving specific municipalities and territories where North Korean agents tend to operate the most. NPFRA singles out the Dalian, Dandong, Jinzhou and Shenyang municipalities in the Liaoning province as well as Hong Kong.[18] Similarly, FIs can create alerts for other "hot spots" based on the available data of proliferation financing cases.

Sixth, filing SARs on any transactions that do not make sense might help uncover proliferation networks, even when FIs cannot identify if transactions are related to proliferation. This is because proliferators hide the end users behind the front companies and convoluted payment schemes.

Seventh, FIs should pay greater attention to transactions that involve the shipping industry. For example, by providing letters of credit to trading networks that assist vessel-to-vessel transfers, FIs inadvertently help North Korea circumvent sanctions. FIs might consider adopting more stringent due diligence procedures and stricter conditions to transactions related to shipping activities in high-risk scenarios.

Finally, FIs might consider amending trade finance service contracts to allow an institution to exit a transaction or a relationship without a penalty if the client does not identify transactions involving the purchase or sale of strategic goods or if there are other concerns about a transaction.



Conclusion

Proliferators are not going anywhere and FIs have a special responsibility in pursuing the common goal—preventing the next nuclear, biological or chemical attack. Proliferation financing risks are harder to grasp and operationalize compared to money laundering and terrorist financing. However, there are steps that FIs can take today to combat proliferators.

Togzhan Kassenova, PhD, CAMS, senior fellow with the Project on International Security, Commerce, and Economic Statecraft (PISCES), Center for Policy Research at University at Albany-SUNY; senior visiting fellow at the Elliot School of International Affairs, George Washington University; nonresident fellow with the Nuclear Policy Program at the Carnegie Endowment for International Peace, Washington, D.C., USA, tkassenova@albany.edu

The author is grateful to Matthew Ingram for his feedback on the earlier draft.

[1] "United States Files Complaint to Forfeit More Than $1.9 Million From China-Based Company Accused of Acting as a Front for Sanctioned North Korean Bank," *United States Department of Justice*, June 15, 2017, https://www.justice.gov/usao-dc/pr/united-states-files-complaint-forfeit-more-19-million-china-based-company-accused-acting

[2] "U.S. v. Funds Associated with Mingzheng International Trading Limited et al.," *United States District Court for the District of Columbia*, June 14, 2017, https://www.courthousenews.com/wp-content/uploads/2017/06/Mingheng.pdf

[3] Alex Wellerstein, "Nukemap," *Missilemap*, https://nuclearsecrecy.com/nukemap/?&kt=10&lat=38.89511&lng=-77.03637&hob_psi=5&hob_ft=2207&psi=20,5,1&zm=13

[4] The gist of the bargain the countries reached under the NPT was that countries with nuclear weapons would eventually disarm while countries without nuclear weapons would get access to peaceful nuclear technology in exchange for their promise not to develop nuclear weapons.

[5] 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.

[6] 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 a good in question may be used in a WMD program.

[7] 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, 85.

[8] "S/2019/171," *United Nations Security Council*, March 5, 2019, https://www.undocs.org/S/2019/171, 52-53.

[9] "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, https://www.fincen.gov/news/news-releases fincen-issues-advisory-iranian-regimes-illicit-and-malign-activities-and

[10] Ibid; UN North Korea Panel of Experts report, 5. 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, https://www.acamstoday.org/2019-u-n-north-korea-panel-of-experts-report-takeaways-for-financial-institutions-2/

[11] "Chinese Man Convicted on Charges of Exporting U.S.-origin Pressure Transducers to Iran," *Iran Watch, Wisconsin Project*, February 9, 2016, https://www.wisconsinproject.org/chinese-man-convicted-on-charges-of-exporting-u-s-origin-pressure-transducers-to-iran/

[12] For discussion on how export controls and proliferation financing controls relate to each other, see Togzhan Kassenova, "Challenges With Implementing Proliferation Financing Controls: How Export Controls Can Help," *WorldECR: the Journal of Export Control and Sanctions*, May 2018, https://carnegieendowment.org/2018/05/30/challenges-with-implementing-proliferation-financing-controls-how-export-controls-can-help-pub-76476; Rachel A. Weise, Gretchen Hund, Geoffrey Carr, "Export Controls and Counterproliferation Finance: Two Sides of the Same Underlying Illegal WMD Activity," *The Nonproliferation Review*, Volume 25, Issue 1-2, 2018, 129-145.

[13] For a range of helpful resources, see the Royal United Services Institute's Counter-Proliferation Finance collection: https://rusi.org/projects/counter-proliferation-finance

[14] "Review of the End User List," *Ministry of Economy, Trade, and Industry*, https://www.meti.go.jp/english/press/2017/0524_001.html

[15] See recommendations from the UN North Korean Panel of Experts, "S/2019/171*," *United Nations Security Council*, 64-65, https://www.undocs.org/S/2019/171.

[16] Ana Alexandre, "HSBC Blockchain Connection Reduces Transaction Time by 40%," *Cointelegraph*, July 10, 2019, https://cointelegraph.com/news/hsbc-blockchain-connection-reduces-transaction-time-by-40

[17] Austin Cook and Beth Herron, "Harvesting Unstructured Data to Reduce Anti-Money Laundering (AML) Compliance Risk," *SAS Institute*, https://www.sas.com/content/dam/SAS/support/en/sas-global-forum-proceedings/2018/2225-2018.pdf.

[18] "National Proliferation Financing Risk Assessment 2018," *U.S. Department of the Treasury*, 18, https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf