Center for a New American Security

July 12, 2018

Testimony before the House Financial Services Committee Subcommittee on Terrorism and Illicit Finance

Countering the Financial Networks of Weapons Proliferation

Elizabeth Rosenberg, Director and Senior Fellow
Energy, Economics, and Security Program, Center for a New American Security

Thank you, Chairman Pearce and Ranking Member Perlmutter, for convening this hearing on countering the financial networks of weapons proliferation and for inviting me to appear before this subcommittee.

The financing of weapons of mass destruction proliferation is a grave threat facing the United States and the global financial system. The ability of rogue states and, potentially, malicious non-state actors to obtain weapons of mass destruction by using illicit financial activity and procurement networks is a major challenge to U.S. foreign policy goals, to the security of our homeland and that of our allies and partners, and to the integrity of the global financial system and the global nonproliferation regime.

Countering proliferation finance must be a core part of the policy approach to the United States' most pressing national security concerns, specifically North Korea, Iran, and Syria. Furthermore, the United States must lead on this issue in international forums such as the United Nations Security Council. This body and several others have taken important, though merely nascent, measures to place obligations on member states to halt proliferation finance. There is broad opportunity for the United States to advance policy and global cooperation on an important security issue, with near-term and meaningful benefits for global nuclear security.

Advancing the critical, even essential, global policy regime to counter the financing of proliferation will feature several primary challenges. First, proliferation finance is difficult to detect. Proliferation networks and specific individuals in these networks leverage the openness and interconnectedness of the global financial and trading system to achieve their malicious goals. For example, in 2013 Spanish authorities intercepted a shipment of corrosion-resistant valves destined for an oil field services company in the United Arab Emirates. Subsequent investigation found that the valves were going to be diverted to Iran for potential use in Tehran's nuclear program.[1] As evident from this case study, the global financial system prizes frictionless transfers of goods and capital, which

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

proliferators have taken advantage of on multiple occasions. Moreover, proliferators have taken advantage of gaps in different national regulatory regimes to evade detection. For example, although paragraph 16 of U.N. Security Council resolution 2321 (2016) requires U.N. member states to limit the number of bank accounts held by DPRK Embassy staff, the U.N. Panel of Experts on DPRK noted that states differed in their interpretation of the range of staff covered by this provision.

Second, countering the financing of proliferation is a highly technical subject, sitting at the intersection of sanctions enforcement, export control, financial crimes compliance, and the global nuclear nonproliferation regime. As these networks operate across multiple jurisdictions, involve an array of different constituencies—with different legal and regulatory authorities, various privacy and data-sharing obligations, and with major differentiation in political will and technical capacity—coordinating a truly effective international response is difficult. Many countries that otherwise lead on financial transparency and nuclear nonproliferation have struggled to summon the political will to tackle proliferation finance head-on, and even where there is political will government authorities and private sector compliance professionals may lack knowledge about how to do this work properly.[2]

It is truly alarming that the community of nations concerned by the threat of nuclear challenges, notwithstanding the ostensible commitment of many nations to this issue through support of multiple U.N. Security Council resolutions, nevertheless pays relatively less attention to the low probability but extraordinary high impact threat—the use of a weapon of mass destruction—than to the threat of a terrorist attack. While larger international financial institutions may have the resources and know-how to examine their transactions for the footprint of financing of proliferation, smaller, regionally-focused banks may not. Indeed, in some cases these smaller institutions may not even be aware of their obligations under international law, particularly if the local regulatory environment is weak.

The undeniable difficulties associated with countering the financing of proliferation, however, should not give the false impression that creating a more effective policy framework is beyond the capacity of the international community. We know the deficiencies in the system, and we can identify strategies to ameliorate them.

To begin with, there are major gaps in the regulatory regime that hamper a better response to this critical issue. Compliance and oversight programs for financial institutions have historically focused on financial integrity threats other than proliferation finance, like anti-money laundering, anti-corruption, and countering terrorist financing. This focus has led to a less-than-optimal outcome for checking the ability of North Korea and Iran, for example, to develop nuclear weapons capabilities. For policy leaders to clarify that counter-proliferation finance is on par with an obligation to counter terrorism will go a long way to raise the profile of this issue and update compliance posture.

Beyond a compliance footing, there are significant expertise and sophistication gaps in tracking proliferation financing not just among banks, but also among jurisdictions. While the United States,

[2] See e.g., Andrea Berger, "A House Without Foundations: The North Korea Sanctions Regime and Its Implementation," Whitehall Report 3-17 (Royal United Services Institute, June 2017), 40, https://rusi.org/sites/default/files/201706_whr_a_house_without_foundations_web.pdf.

the United Kingdom, and other European countries like France and Belgium have invested in building the institutional and intellectual capital needed to understand and counter this threat, many vulnerable jurisdictions such as Hong Kong or Malaysia have only recently begun to do so, and many more jurisdictions have not yet faced the issue. These countries will require more education and technical assistance, which the United States and a few in Europe, as well as Australia, are well positioned to provide. Some U.N. agencies offer workshops on proliferation financing (often together with terrorist financing), funded by countries such as Canada and Japan. Capacity building is important: as proliferation finance networks operate globally, and are quite adaptable, international efforts to combat them are only as strong as the weakest jurisdiction.

Given the size and reach of the U.S. financial system, as well as the sophistication of the legal and regulatory tools at the disposal of U.S. officials, Washington's policymakers must lead the way on disrupting the financing and procurement of weapons of mass destruction. U.S. policy leadership will yield numerous dividends. Not only will better regulation of the U.S. financial system foreclose avenues of proliferation finance in the United States, and via the U.S. dollar anywhere else in the world, but it will also offer important models for other jurisdictions to follow. Better U.S. rules can serve as standards of excellence for other jurisdictions and for financial institutions around the world. Global regulators and banks already look to the United States as the regulatory standard-setter for numerous aspects of the international financial system. A strong counter proliferation finance regime must be a part of that.

Expanding Mechanisms for Information Sharing

Perhaps the most significant policy adaptation that will help to counter the financing of proliferation is the crafting of better mechanisms for the timely collection and dissemination of information. Governments and banks must be able to share relevant information with one another or risk regularly, if unwittingly, facilitating the financing of proliferation. Banks must be able to widely, though securely and with appropriate data protections, share the information they collect relevant to proliferation finance through their routine business operations. Because most proliferation networks extend across multiple countries, individual jurisdictions, enforcement agencies, and financial institutions can acquire only a partial view of any one proliferation network. In one example of a prominent North Korean proliferation network, the web of trusted associates had operational nodes in China, Hong Kong, Malaysia, and Singapore.[3] Ensuring that policymakers can create the regulatory framework, nationally and internationally, to connect these partial perspectives, and thus successfully map international networks, will be critical to addressing this threat.

There are examples for information sharing in U.S. law that Congress, the administration, and U.S. allies and partners can build on. Sections 314 (a) and 314 (b) of the USA PATRIOT Act can serve as models for creating the operational ability to facilitate information sharing both between government and financial institutions and between financial institutions. These approaches, though, are only starting points. Many stakeholders claim significant concerns around different privacy regimes that prevent seamless sharing of information across national borders. Policymakers should

[3] Jonathan Brewer, "The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation" (Center for a New American Security, January 2018), 7, https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-ProliferationFinance-Finalb.pdf?mtime=20180202155127.

identify how to harmonize privacy regulations so that justifiable concerns about misuse of personal data do not prevent cooperation on an important law enforcement and international security priority.[4]

Better information sharing and data analysis tools can make the most of the data the U.S. government and counterparts already collect. Suspicious Activity Reports (SARs) generated by banks across the world for their regulators are an important source of insight into global proliferation finance networks. Congress should explore the development of new ways to gather and analyze this data in order to aid investigators in uncovering proliferation finance networks. There are new technology tools, including the application of machine learning and artificial intelligence methodologies, that may be of use. The United States can pilot fusion cells of experts with access to SAR and other relevant data (such as shipping data, travel records, or other sources) to experiment with new methodologies and technology for uncovering proliferation finance.

If policymakers pursue better information sharing mechanisms, or data analytics, solely in the United States, however, their effectiveness will be limited. Proliferation finance networks can span multiple jurisdictions so other major financial centers like Hong Kong, or major proliferation conduit jurisdictions such as Malaysia and Singapore, will need to adopt similar approaches to ensure the timely collection and use of information. It is encouraging that important U.S. partners, like the United Kingdom, are pioneering their own efforts to facilitate the sharing of sensitive information through its Joint Money-Laundering Intelligence Taskforce (JMLIT). Many jurisdictions have only started to work on how to incorporate best practices from these efforts into their own local policy and regulatory framework.

U.S. technical assistance can play a critical role in a process of replicating successful information sharing or analytical processes. Observers around the world have highlighted the utility of efforts by the U.S. Export Control and Related Border Security (EXBS) and the Defense Threat Reduction Agency (DTRA) programs to-date. The U.S. government should encourage and prioritize the provision of technical assistance to counterparts in jurisdictions with less-developed proliferation finance controls to expand relevant data and typology gathering, and strategies for producing proliferation-related red flags and SARs. Congress has an important role to play in funding and overseeing this strong and effective work. Legislators concerned with a comprehensive and successful approach to addressing North Korean and Iranian proliferation concerns, for example, must focus on proper resourcing and funding for these initiatives.

The Need for More Awareness-Raising

As previously noted, many countries and firms exposed to proliferation finance risk are unaware of this threat and their legal obligations to counter it. The U.S. government can foster efforts to better counter proliferation finance by offering more information to the public about the dangers facing the global financial system. Advisories by the Financial Crimes Enforcement Network (FinCEN) are invaluable in educating a wide variety of financial and legal sector stakeholders about threats to the

[4] See e.g., Andrea Berger and Anagha Joshi, "Countering Proliferation Finance: Implementation Guide and Model Law for Governments," Guidance Paper (Royal United Services Institute, July 2017), 23, https://rusi.org/sites/default/files/201707_rusi_cpf_implementation_guide_and_model_law_berger_joshi_0.pdf.

global financial system. By making more information available to financial institutions and outside experts, policymakers can also help create a virtuous cycle. More information from the government will lead to more useful and targeted detection of proliferation finance from the banks, which, in turn, will lead to even better information shared by the government. This entire process will lead to stronger law enforcement outcomes to counter proliferation finance and a stronger deterrent to proliferators to engage in this illicit activity in the first instance.

Policymakers must do more to release information about proliferation finance typologies to the public and key financial institutions and counterpart regulators. Outside experts have conducted useful work in this space that has significantly informed financial institutions' approach. Dr. Jonathan Brewer's "Study of Typologies of Financing of WMD Proliferation" serves as a valuable example of private study of these networks.[5] Similarly, the reports of the United Nations Panel of Experts created pursuant to Resolution 1874 have shone a light on global proliferation networks and offered an invaluable stream of information to banks seeking to shut these networks out of their institutions.[6] However these efforts are partial. Policymakers can significantly augment them by disclosing greater information about typologies of the financing of proliferation either in the public domain or through classified or private networks.

Law Enforcement and Disruption of Proliferation Finance Networks

Law enforcement will play a key role in any successful framework to counter proliferation finance. Over the past eight years, due to the attention paid to Iran and North Korea as proliferation threats, the U.S. law enforcement community has garnered an international reputation for its ability to investigate, disrupt, and prosecute those who operate proliferation finance networks. These professionals have unique strengths in asset tracing, compiling of typologies to dissect how proliferation finance networks have operated, and identifying shell companies to learn the true beneficial owner behind proliferation activities.[7]

Often, disruption of facilitation, including financial facilitation, networks is the preferred strategy of U.S. law enforcement officials when they are involved in work to counter proliferation. This is the case because many of the criminal actors in proliferation networks reside in jurisdictions outside of the reach of U.S. criminal prosecution. Asset seizure or forfeiture may also be an effective tool to raise the cost of doing this illicit business. Of particular utility are civil asset forfeiture authorities, and the 981(k) provisions which allow the United States to restrain, seize, and forfeit funds held in

---

[5] Brewer, "Study of Typologies of Financing of WMD Proliferation, Final Report."
[6] See especially "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," United Nations Security Council (UN document S/2017/150), February 27, 2017, https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/s_2017_150.pdf and "Report of the Panel of Experts established pursuant to resolution 1874 (2009)," United Nations Security Council (UN document S/2018/171), March 5, 2018, https://www.securitycouncilreport.org/atf/cf/%7b65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7d/s_2018_171.pdf.
[7] See, for example, the Department of Justice's investigation of Dandong Hongxiang Industrial Development Co. Ltd. (DHID). "Four Chinese Nationals and China-Based Company Charged with Using Front Companies to Evade U.S. Sanctions Targeting North Korea's Nuclear Weapons and Ballistic Missile Programs," United States Department of Justice, September 26, 2016, https://www.justice.gov/opa/pr/four-chinese-nationals-and-china-based-company-charged-using-front-companies-evade-us.

foreign bank accounts located abroad by seizing an equivalent amount of funds in correspondent bank account of that foreign financial institution located in the United States. Put another way, this provision allows U.S. law enforcement to disrupt criminal activity even in jurisdictions with which the United States does not have extradition treaties. Here too international efforts will be important. In other jurisdictions authorities have faced difficulties and delays in carrying out seizures and freezes quickly.[8]

Financial System Transparency

Congress has a direct role to play in improving the legal and regulatory framework to counter proliferation finance. As a first priority, Congress should increase transparency in the financial system, and there must be no anonymous companies. This work is essential to arresting the ability of illicit proliferation networks to abuse our financial system to advance their dangerous work.

The recent introduction of H.R. 6068, "the Counter Terrorism and Illicit Finance Act," can be a step forward in reform of the Bank Secrecy Act to empower the administration to put in place strong counter proliferation finance strategies. It allows the sharing of suspicious activity reports within a financial group across international borders. However, in providing an 18-month safe harbor for violations of the customer due diligence rule it walks back existing supervisory expectations according to which regulators have been citing banks for years. It is indeed important to encourage financial institutions to self-report without fearing harsh legal action, but lawmakers must not water down existing practices related to customer due diligence, particularly the need to clearly determine customer activity and risk profile, that are so important—and must be built upon--to preventing illicit finance and abuse of the financial system.

Beyond this legislation Congress should partner with enforcement authorities to create incentives for U.S. financial institutions to innovate in their countering proliferation finance practices. Offering safe harbor from enforcement liability for financial institutions that demonstrate innovative approaches in their financial integrity controls is one potential incentive. Currently, the Bank Secrecy Act contains safe harbor from civil liability for Suspicious Activity SARs and Section 314 disclosures. Congress should ask the U.S. Treasury Department to develop safe harbor options to spur banks to allocate greater resources to information sharing and more effective analysis. The Financial Services Information Sharing and Analysis Center (FSISAC), which provides shielding and liability protection to members from certain regulatory requirements such as the Freedom of Information Act (FOIA), offers one model. While less beneficial to banks, Justice Department Cooperative Agreements may be another way in which financial institutions can receive credit for their cooperative efforts with government. Regulatory "sandboxes" that allow experimentation in countering proliferation finance while shielding institutions from liability are yet another means to incentivize private-public collaboration.

Given the importance of greater transparency to effectively counter proliferation finance, it is regrettable that Congress has not acted more swiftly in requiring complete and total disclosure of beneficial ownership information in regulations governing corporate entity creation. There must be no anonymous companies in the United States. While the report to be generated under Section 10 of

[8] Berger, "A House Without Foundations."

H.R. 6068 would provide useful information about how criminal investigators use the limited beneficial ownership information they currently collect, the requirements of the bill do not spur any immediate action to cut off proliferators and other illicit actors from the ability to create innumerable shell and front companies to disguise their criminal activity. If countering North Korea's and Iran's proliferation networks are truly top priorities of this Congress, legislators should consider requiring more concrete action on beneficial ownership in the short term.

Congress should also expand the amount of information required in financial payment messages. Lawmakers should also initiate a formal process with international counterpart parliamentarians to push for complementary requirements abroad. Many proliferators, along with other criminals, omit information incident to a transaction, and these data are only verified in a limited manner. Additionally, proliferators often use open account trade transfers, which, compared to letters of credit, convey only the most basic information about the purposes of a transaction and the parties involved, and which can often be falsified. The amount of information required in payment messages currently is insufficient to assist with countering proliferation finance investigations and to realistically protect financial system integrity.

Deepening Oversight of Non-Bank Commercial Institutions

In practice, the current countering proliferation finance regime relies on bank compliance to generate actionable intelligence. In particular, it does not well integrate other sources of trade or shipping data which could clarify and present opportunities for interdiction earlier in the supply chain. At present, banks may be able to eventually track proliferation products through retroactive investigation of transaction data, but they have virtually no ability to catch or interdict this commerce in real time. Shifts in the conduct of global trade finance, in particular the shift from letters of credit to open account transactions—have exacerbated this reality. The chance for disrupting proliferation finance exists when proliferation activities are identified before the final exchange of money and goods, which is difficult to do with open account transfers. Additionally, the amount of information conveyed is much less with open account transfers as compared to trade finance funded transactions.

U.S. policymakers can spearhead changes in global trade practices that may diminish the window of opportunity for proliferation networks. Today, the lack of standardized classification of goods and information included in trade and shipping documents is an information gap that both banks and governments confront. Too often inconsistent labeling can allow proliferation goods to slip through import-export controls. In my research on proliferation finance I have found that banks say these inconsistencies make it difficult to move with certainty in flagging suspicious trading activity. Closing this information gap by standardizing the taxonomy for goods within and across jurisdictions will ensure better customs compliance and enforcement, including through machine-driven screening and analytics across data sets, and it will help prevent labeling which obscures the real products being shipped.

In addition to the problem of labeling inconsistency, another core challenge to countering proliferation finance work associated with trade and shipping data is the inadequate supply of such financial documentation to banks. At present, regulatory requirements or cross-industry data-sharing mechanisms do not exist to close this gap. However, many stakeholders note that more, and more

consistent, trade information could provide critical insight for financial institutions screening, analyzing, and ideally disrupting, proliferation-linked transactions and networks. More cross-industry information sharing and more information in payment messages, both mentioned previously, can help address this issue.

The U.S. Presidency of the Financial Action Task Force (FATF), which began on 1 July 2018, is an invaluable opportunity for the United States to promote these critical issues within the framework of FATF, and to leave as its legacy a global financial system significantly strengthened against the threat of proliferation financing.

Working with U.S. allies and partners

Almost all global financial centers, particularly those in East Asia at the front lines of countering North Korean proliferation activities, are only beginning to acknowledge and understand the nature of the proliferation finance threat. Many of these jurisdictions are contemplating how to issue guidance on proliferation finance based on their own experiences with investigations and collection of data from SARs, as well as the development of information sharing mechanisms based on models used in the United States and the United Kingdom.

Financial institutions the world over will be key partners for policymakers in identifying the financing of proliferation. Institutional risk assessments will help inform this process and large, international banks who can do this work should pursue it aggressively and model it for smaller, regional banks who are at high risk. The increased use of risk assessments will be to the advantage of the non-proliferation regime, and the big banks, who have correspondent relationships with the smaller banks. As a result, it will make the whole system safer. The U.S. Congress can raise the flag on this issue in oversight of the executive branch and in the statements members make on how policymakers in the United States and abroad should address proliferation finance.

I want to close by stating how important it is for governments and financial institutions to avoid complacency over operations that might implicate North Korean and Iranian proliferation interests. The broader financial services and national security communities must understand that compliance with sanctions is insufficient on its own to counteract the activities of proliferation finance networks or to safeguard the integrity of the global financial system. The consequences for failing to appreciate the seriousness of the threat are real. International financial institutions face risk of expensive enforcement measures and the reputational harm that would come from facilitating transaction by rogue states. Governments face the risk of being the weak link that gives a WMD capability to a U.S. adversary. The stakes could not be higher.

Thank you for your time and attention. I look forward to your answering your questions.