Challenges with implementing proliferation financing controls: How export controls can help

Why do financial institutions struggle to implement proliferation financing controls? Would looking at proliferation finance challenges as an export control matter help in the fight against the proliferators? Togzhan Kassenova suggests it's time to rethink what we think about how to address proliferation finance challenges.

'We only catch the dumb ones.' That is what the risk manager of a major bank tells me when I ask about banks' ability to detect illicit financial transactions.[1] Detecting proliferation-relevant illicit financing is even harder than detecting money laundering or terrorism financing. Governments and financial institutions around the world have been dealing with money laundering and terrorism financing for decades. They have developed typologies, 'red flags', and standard operating procedures to minimise exposure to money laundering or terrorism financing. Compared to money laundering and terrorism financing, proliferation financing is a relatively recent and less understood challenge.

The risks posed by weapons of mass destruction ('WMD') stem not only from ready-made bombs, nuclear, chemical, or radiological material, but from dual-use goods and technology that are traded, shipped, and used globally. Laptops, transistors, instant coffee – almost every single moment, no matter where you find yourself in the world, you are surrounded by products that rely on the same technology and material as weapons of mass destruction. Semi-conductor material that is indispensable for laptops and transistors can be used in military equipment. Production of instant coffee, as well as of dry ice-cream for astronauts, relies on freeze-drying technology that can be used in bio-warfare research. Components for nuclear power reactors that generate electricity rely on dual-use components and technology that can be used in a nuclear weapons programme.

This article explains why financial institutions struggle with implementing proliferation financing controls. The limitations that financial institutions face do not remove responsibility from them to do better, and there are steps they can take to strengthen their capacity to prevent and detect proliferation activities. Additionally, there is untapped potential for cooperation between financial institutions and other actors, including export control authorities.

To date, proliferation financing controls have mostly been seen as an 'add-on' to anti-money laundering and counter-terrorism financing measures. Looking at proliferation financing challenges as related to export control efforts can significantly improve the overall capacity of a given country to minimise proliferation financing risks. In this article, proliferation financing controls refer to measures designed to prevent financing of WMD-related activities.[2]

UN Security Council country-specific sanctions versus broader proliferation concerns[3]

A common perception within the private financial sector is that proliferation financing controls refer to the implementation of country-specific sanctions – for example, those designed to prevent North Korea ('DPRK') and

Iran from tapping into the global financial system for proliferation support. However, country-specific sanctions should be seen as integral but *not the only* part of proliferation financing controls.

Financial institutions struggle with implementing both country-specific sanctions and broader proliferation financing controls. This is because financial institutions understand better and internalise more easily country-specific sanctions, while broader proliferation risks appear more abstract to the institutions and they find themselves ill-equipped to address those risks.

There follows a description of specific challenges that financial institutions face when implementing country-specific sanctions and broader proliferation financing controls.

Challenges in implementing UN country-specific sanctions

Resolutions adopted by the UN Security Council ('UNSC') under Chapter VII of the UN Charter impose obligations on all UN member-states to implement UN sanctions. Financial institutions are aware of UN Security Council resolutions ('UNSCRs') though they are not always well equipped to implement country-specific ones. In the proliferation realm, Iran- and DPRK-specific sanctions are especially relevant.[4]

In the wake of the 2015 Joint Comprehensive Plan of Action ('JCPOA' or 'Iran Nuclear Deal'), the UN Security Council rolled back UN nuclear sanctions. Previously, financial institutions were prohibited from conducting business with entities and individuals designated by the UN Security Council. Financial institutions were banned from providing their services for prohibited activities (e.g., activities that could contribute to Iran's enrichment-related, reprocessing or heavy water-related activities, or to the development of nuclear weapon delivery systems). Iranian banks could not open new business in other countries if the business was connected with prohibited activities. The UN Security Council imposed a broad requirement on countries to exercise vigilance over business potentially connected with prohibited activities.[5]

Following the Iran Nuclear Deal, the UN Security Council reduced the list of designated entities and individuals. The UN Security Council obligates countries to seek its approval for financing of UNSC-approved procurement by Iran. It dropped the broad requirement on countries to exercise vigilance over business potentially connected with prohibited activities.[6]

In contrast to its rollback of sanctions related to Iran's nuclear programme, the UN Security Council continued to expand sanctions against the DPRK in response to its audacious WMD programme.

The financial provisions of DPRK sanctions are broad. For example, UNSCR 2270 (2016) introduces activity-based and category-based targeted financial sanctions. It requires countries to prevent financial transactions related to DPRK's nuclear or ballistic missile programmes or other prohibited activities. The same resolution bans the opening and operation of branches and subsidiaries of DPRK banks; bans public and private financial support for DPRK's prohibited activities; and requires the freezing of assets and economic resources, which include transportation vessels. UNSCR 2371 (2017) prohibited new or expanded joint ventures and cooperative commercial entities with the DPRK. UNSCR 2375 (2017) went further and prohibited all joint ventures, cooperative entities, and expansion of existing joint ventures with DPRK entities and individuals.[7]

Some countries lack the legal basis to deal efficiently with implementing sanctions because their institutions are not authorised to take relevant actions.

Below are five examples of challenges that financial institutions face with implementing country-specific sanctions.

First, domestic legislation in many countries around the world does not fully internalise UN sanctions. That means some countries lack the legal basis to deal efficiently with implementing the sanctions because their institutions are not authorised to take relevant actions – e.g., denying financing, freezing assets, or punishing violators.

The second and related challenge is an inefficient process for updating domestic regulations and informing the private sector promptly to match changes in UN designations of entities and individuals. For example, if the UN Security Council designated new entities or individuals as proliferators, but a given country failed to update its lists, financial institutions might continue conducting business with those entities and individuals during this lag time.

The third challenge pertains to practicalities. Financial institutions use software that screens transactions against the lists of UN-designated entities and individuals. In practice, such screening system returns a high number of false positives, often thanks to similar or similar-sounding names. Screening results that return 95% false positives are not unusual. Risk managers spend a lot of time dealing with false positives and writing up reports on each case; time and effort that could be spent on more efficient risk-management procedures.

The fourth challenge for financial institutions is the difficulty with identifying sanctioned countries, entities, and individuals or their middlemen behind transactions. Since list-based screening is not fool-proof, financial institutions have to find other ways to make sure they are not servicing sanctioned countries, companies, people or the front

companies that work on these countries' behalf. This is difficult to do because of proliferators' deceptive practices.

The DPRK represents the most notorious example of challenges. North Korea has perfected the art of disguise and employs various tricks to hide its identity when interacting with the global financial institutions. The Kim Jong-un regime relies on the help of DPRK procurement managers who reside in third countries or middlemen from these countries who act on behalf of the DPRK. These middlemen use multiple bank accounts under different names and pay for goods in several instalments to muddy transactions.[8] In one of the numerous examples that has come to light, a representative of the designated DPRK Daedong Bank opened several accounts in mainland China and Hong Kong, both in his name and in the name of front companies, and used those accounts to carry out transactions worth millions of US dollars.[9]

Because of such deceptive practices, the DPRK does not feature on the documentation that financial institutions receive. As a result, often financial institutions do not know who they are dealing with.

Finally, the underlying challenge to sanctions implementation is the limited capacity of financial institutions to distinguish proliferation activity. DPRK sanctions require activity-based controls which means that financial institutions are supposed to prevent transactions related to prohibited activities but banks, in general, are not in the best position to identify such transactions. Financial institutions see only a small part of data related to a given transaction, and they do not have the technical expertise to distinguish what is proliferation-relevant and what is not.

To put it in perspective, even customs officers who deal with actual goods on an everyday basis often struggle to distinguish dual-use items. However, in contrast to financial institutions, customs officers have access to more information on any transaction, specifically related to the goods involved, and officers can physically inspect the items. There are also procedures in place for customs officers to seek technical expertise from relevant authorities when needed for determining the nature of goods.

Compared to government agencies who deal with controlled goods on a regular basis, such as customs or export licensing authorities, financial institutions will unlikely ever be fully equipped to determine the nature of a transaction – whether it is related to prohibited activities or not – without external help.

Having said this, financial institutions cannot afford to recuse themselves from carrying their share of responsibility. They should be concerned with doing better both for the common good (international security) and for self-serving reasons (to avoid reputational risks and punishment).

Financial institutions see only a small part of data related to a given transaction, and they do not have the technical expertise to distinguish what is proliferation-relevant and what is not.

On this last point, the role of the United States in relation to non-US banks is especially relevant. Foreign banks rely on the US financial system to clear transactions in US dollars. Losing access to the US financial system carries serious repercussions for foreign banks.

The US government has shown readiness to hit foreign banks for proliferation-related activities. In one example, in 2017, under the USA Patriot Act, the US Treasury labeled China's Dandong Bank an 'institution of primary money laundering concern' for carrying out transactions on behalf of North Korea, effectively cutting it from the US financial system.[10] In another recent example, the Trump administration issued an executive order that allows the US Department of Treasury to impose sanctions on foreign banks that 'knowingly conducted or facilitated any significant transaction in connection with trade with North Korea'.[11]

While the limitations facing financial institutions in identifying transactions of proliferation concern cannot be fully eliminated, they can be mitigated. Guidance provided by governments and the Financial Action Task Force ('FATF'),[12] employment of 'red flags', and proliferation finance typologies[13] are of great value and should be incorporated into risk management practices of financial institutions.

Moreover, education of compliance officers, including on how to access relevant information from non-government sources, would further help to sensitise them to proliferation finance risks. Academic institutions and think-tanks, such as Royal United Services Institute ('RUSI'), the James Martin Center for Nonproliferation Studies, Project Alpha at King's College London, the Center for New American Security ('CNAS') to name but a few, offer timely analysis of proliferation trends and provide practical suggestions for financial institutions on how to strengthen proliferation financing controls.[14]

On the opposite side of the spectrum, there are certain potentially negative implications associated with over-compliance and de-risking when it comes to country-specific sanctions. For example, some financial institutions avoid doing any Iran-related business altogether, despite the lifting of nuclear sanctions in the aftermath of the Iran Nuclear Deal. Over-compliance and de-risking can negate the effectiveness of sanctions and bring unintended consequences. In the case of Iran, the reluctance of global financial institutions to engage can reduce political support for the deal within the country.

Challenges of implementation – broader proliferation context

Proliferation financing controls cannot be tied solely to country-specific sanctions implementation. Proliferation risks expand further than those emanating from specific countries, such as the DPRK or Iran. New proliferator countries can appear on the horizon, or non-state actors, such as terrorist organisations, can attempt to obtain proliferation-sensitive goods. Our reliance on dual-use goods and technology in daily life means that every day and in every part of the world goods that can be misused for weapons purposes are easily available. Determined proliferators can abuse legitimate trade and financial systems to achieve their aims.

To counter this risk, the UN Security Council passed a resolution in 2004 that obligated all UN member-states to

implement proliferation controls that would prevent non-state actors from acquiring WMD. UNSCR 1540 (2004) includes provisions that call on UN member states to adopt and enforce laws which would prevent financing of WMD-related activities by non-state actors and enact export controls related to financing the movement of sensitive goods.[15] More recently, UNSCR 2325 (2016) called on countries to pay greater attention to proliferation finance measures.[16]

Financial institutions are typically not well attuned to wider proliferation trends, risks, and states' responsibilities under broader proliferation-relevant UN Security Council resolutions. So far, the author has not encountered representatives of financial institutions who are aware of UNSCR 1540.

Financial institutions are not usually familiar with the concept of dual-use goods and technology and struggle to internalise what proliferation entails.

Even though financial institutions face challenges when implementing sanctions, compared to broader proliferation financing controls, the implementation of country-specific sanctions is more structured, is associated with more concrete measures, and guidance is more explicit, especially when it comes to targeted financial sanctions aimed at designated entities and individuals. UNSCR 1540, by design, leaves the interpretation of national compliance relatively broad, without setting firm benchmarks.

Broader proliferation risks are harder for financial institutions to grasp and even harder for them to address. The majority of countries around the world have limited awareness of proliferation and proliferation trends. Many decision-makers mistakenly think that WMD proliferation refers to the spread of actual weapons of mass destruction and their components, without realising that strategic goods and technology are directly relevant to WMD risks. Moreover, many developing countries do not think WMD proliferation poses risks to their security and prefer to use their limited resources pursuing other national priorities.

Not surprisingly, many countries lack legal and regulatory frameworks for implementing proliferation financing controls, which is a more advanced component of WMD nonproliferation policy. As a result, financial institutions are not usually familiar with the concept of dual-use goods and technology and struggle to internalise what proliferation entails.

On a more practical level, when attempting to identify transactions involving proliferation-relevant goods, financial institutions encounter the following challenges.

Even if financial institutions run checks against HS codes that are associated with sensitive goods, they cannot be certain they catch potentially dangerous transactions. Proliferators can misrepresent product descriptions and use incorrect HS codes in their paperwork. Proliferators can also seek goods that are below the 'controlled goods' threshold – for example, goods with technical characteristics that are slightly lower than those of controlled equipment. There is also 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.

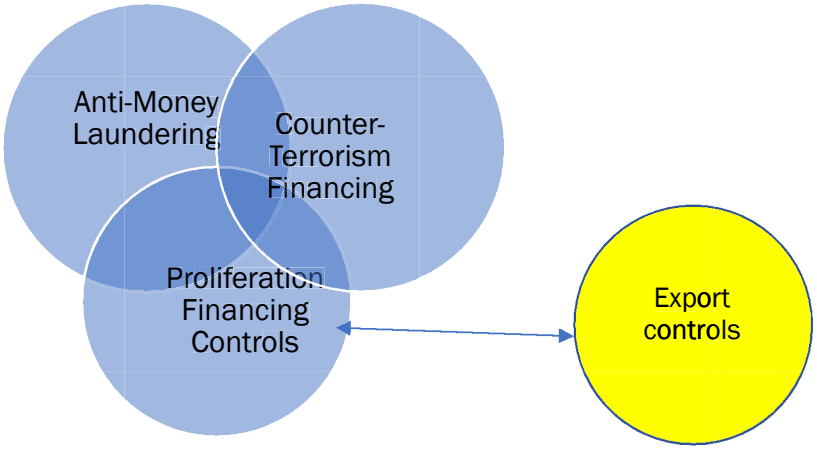
The fact that financial institutions often do not have access to full end use and end-user information is another practical challenge. Who is the final beneficiary? And what is the real purpose of a transaction? These are the kind of questions that financial institutions struggle to answer. Moreover, because financial institutions have not internalised proliferation concerns, the know-your-customer and due diligence procedures do not incorporate checks against proliferation-relevant risks.

Financial institutions also face industry-specific challenges, for example, with data-sharing due to liability and confidentiality rules. Financial institutions can submit suspicious activity reports ('SARs') when they suspect illicit behaviour, but they cannot easily share information on suspicious transactions and customers, even with their branches located in other countries. This means that data that could point to proliferation networks is fragmented and not available in its entirety for analysis.

Another fundamental weakness with implementing proliferation financing controls lies in the isolation of financial institutions from other relevant national actors. It is not general practice for financial institutions to interact with export control agencies, customs, border control, and intelligence authorities. Often, interaction and information flow with law enforcement and intelligence authorities, including financial intelligence units, is one-way. Financial institutions submit SARs to financial intelligence units, but they do not receive feedback on whether and how that data fits into uncovering financial crimes or sanctions violations.

Financial institutions also provide relevant data to law enforcement authorities on demand on specific cases under investigation. This means that opportunities for information exchange that could be mutually helpful to all actors are not fully utilised.[17]

A strong case can be made for



connecting efforts to counter proliferation financing with export controls.[18] Export control licensing authorities have expertise in dual-use goods, and they deal with companies involved in strategic trade. They have information on export licence approvals and denials, 'blacklists' of violators, and other pieces of valuable data. Similar to licensing authorities, customs has more information on products that are traded and shipped across borders than banks ever will. Customs and border control agencies sit on enforcement data that add another dimension to a broader picture of attempts to move goods illegally. Intelligence agencies collect and analyse data not readily available to any other government actors.

Financial institutions also have something to offer to government agencies. Financial institutions cannot disclose proprietary information, but they can share their observations on trends of illicit activities in the financial realm that can add a valuable missing piece to the puzzle of how proliferation networks operate.

In the last few years, several countries established private-public partnerships to deal with financial crimes. In 2016, the United Kingdom launched the Joint Money Laundering Intelligence Taskforce ('JMLIT'). JMLIT analyses data supplied by the public and private sectors to better understand how money launderers and terrorists exploit British financial sector.[19] In 2017, Australia launched Fintel Alliance to combat money laundering and terrorism financing, Hong Kong launched a 12-month pilot project named Fraud and Money Laundering Intelligence Taskforce ('FMLIT'), Singapore launched the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership ('ACIP').[20]

Currently, these private-public partnerships do not focus on proliferation financing. However, proliferation financing controls can be integrated into the agenda of a public-private taskforce that deals with anti-money laundering and terrorism financing. Alternatively, a similar public-private partnership model that includes export control and counter-proliferation authorities can be used to deal with proliferation prevention. In its Guidance on Private Sector Information Sharing (2017), FATF explicitly mentions existing public-private partnerships as valuable platforms for information-sharing.[21] A recently released FATF Guidance on Counter Proliferation Financing (2018) calls for information sharing among public authorities and for government authorities to have a coordinated approach in communicating with the private sector.[22]

Creating opportunities for relevant government actors and the private sector to meet regularly and exchange information would allow all participants to have a more holistic

Links and notes

[1] This article is based on interviews with representatives of financial institutions in several countries over the period of 2017-2018.

[2] There is no universally accepted definition of proliferation finance. The Financial Action Task Force ('FATF'), an intergovernmental organisation established in 1989, provides the following definition: 'The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.'

[3] Some countries implement additional sanctions. This paper focuses on implementation of UN Security Council sanctions.

[4] For a comprehensive list of all financial prohibitions in Iran- and DPRK-focused sanctions, please refer to FATF Guidance on 'Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction,' FATF, 28 February 2018, pp. 42-64.

[5] UN Security Council Resolution 1737 (2006).

[6] UN Security Council Resolution 2231 (2015).

[7] UN Security Council Resolution 2270 (2016), UN Security Council Resolution 2371 (2017), UN Security Council Resolution 2375 (2017).

[8] Final report of the Panel of Experts submitted pursuant to resolution 2345 (2017), 5 March 2018, http://www.un.org/ga/search/view_doc.asp?symbol=S/2018/171, pp. 59-79.

[9] Final report of the Panel of Experts submitted pursuant to resolution 2276 (2016), 27 February 2017, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150, p. 23.

[10] Brett Wolf, 'US Treasury Targets Chinese Bank Over Purported Ties to North Korea, New Sanctions Risk Emerges,' Reuters, 6 July 2017, https://www.reuters.com/article/bc-finreg-chinese-banks-north-korea/u-s-treasury-targets-chinese-bank-over-purported-ties-to-north-korea-new-sanctions-risk-emerges-idUSKBN19S09B; 'Treasury Acts to Increase Economic Pressure on North Korea and Protect the US Financial System,' 29 June 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0118.aspx.

[11] 'Presidential Executive Order on Imposing Additional Sanctions with Respect to North Korea,' 21 September 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-imposing-additional-sanctions-respect-north-korea/.

[12] FATF Guidance on 'Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction,' FATF, 28 February 2018, http://www.fatf-gafi.org/publications/financingofproliferation/documents/guidance-counter-proliferation-financing.html.

[13] 'Typologies Report on Proliferation Financing,' FATF, 18 June 2008, http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html; Jonathan Brewer, The Financing of Nuclear and other Weapons of Mass Destruction Proliferation, CNAS, 24 January 2018, https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation.

[14] For extensive treatment of the challenges with implementation of proliferation financing controls and proposals on how to deal with them, see Jonathan Brewer, 'The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation,' CNAS, 2018; Andrea Berger and Anagha Joshi, 'Countering Proliferation Finance: Implementation Guide and Model Law for Governments,' RUSI, 2017; Jonathan Brewer, 'Study of Typologies of WMD Proliferation,' Alpha Project, King's College London, 2017; Eda Erol and Leonard Spector, 'Countering North Korean Procurement Networks Through Financial Measures: The Role of Southeast Asia,' James Martin Center for Nonproliferation Studies, 2017.

[15] UN Security Council Resolution 1540 (2004), http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540(2004).

[16] UN Security Council Resolution 2325 (2016), http://www.un.org/ga/search/view_doc.asp?symbol=S/RES/2325(2016).

[17] For relevant discussion see FATF Best Practices paper 'Sharing Among Domestic Competent Authorities Information Related to the Financing of Proliferation,' March 2012, http://www.fatf-gafi.org/publications/fatfrecommendations/key/bestpracticespaperonrecommendation2sharingamongdomesticcompetentauthoritiesinformationrelatedtothefinancingofproliferation.html.

[18] For FATF's treatment of the subject, refer to 'Combating Proliferation Financing: A Status Report on Policy Development and Consultation,' FATF, February 2010, http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf, pp. 6-8; FATF Guidance on 'Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction,' FATF, February 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf, 56 (c), p. 22.

[19] 'Joint Money Laundering Intelligence Task Force,' http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit.

[20] 'Fintel Alliance Launch,' Austrac, http://www.austrac.gov.au/fintel-alliance-launch; 'Fraud and Money Laundering Intelligence Taskforce Launched,' Press Release, Hong Kong Monetary Authority, http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml; CAD and MAS Partner 'Industry Stakeholders to Fight Financial Crimes,' http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/CAD-and-MAS-Partner-Industry-Stakeholders-to-Fight-Financial-Crimes.aspx.

[21] 'Private Sector Information Sharing,' FATF, November 2017, http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf.

[22] FATF Guidance on 'Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction,' FATF, February 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf, 59 (a), 59 (c), pp. 24-25.

picture of proliferation trends and risks. The overall objective should be avoidance of stove-piping the responsibilities that each actor carries in preventing proliferation.

The way forward

How can the challenges in implementing proliferation financing controls described above be addressed?

They can be addressed at two levels: the internal level for financial institutions and the external level of collaboration between financial institutions and other actors.

At the internal level, financial institutions would benefit from investing in three key areas – risk-management practices, education of compliance officers, and technical solutions. Risk-management practices should incorporate proliferation risk indicators, similar to anti-money laundering and counter-terrorism financing components. Financial institutions should look out for potential proliferation risks during know-your-customer and due diligence procedures, keeping in mind that proliferators use deception techniques.

Financial institutions should create opportunities for their compliance officers to address a broader context of proliferation trends and encourage them to fully utilise resources offered by both government and non-government players (national authorities, FATF, academic institutions, and think-tanks).

On the technical level, financial institutions would benefit from moving towards more intuitive electronic platforms that go beyond mechanical list-based screening for designated entities and individuals. Some private sector actors have already started developing advanced software that utilises network analysis and artificial intelligence. Incorporating data from sources beyond the financial sector (e.g., export control authorities, law enforcement, and intelligence) would allow financial crimes to be spotted more efficiently.

The most promising path forward lies at the collaborative level. There is a significant untapped potential in public-private partnerships based on the models described above (JMLIT and others). A public-private partnership focused on proliferation finance controls can be a taskforce consisting of representatives of major financial institutions, financial intelligence units, financial regulators, customs, and export control authorities.

Above all, proliferation financing controls should be seen as connected to export controls. Financial institutions would be in a much stronger position to deal with proliferation financing if their efforts go hand in hand with efforts to control flows of sensitive goods.

Togzhan Kassenova is a fellow in the Nuclear Policy Program at the Carnegie Endowment. She works on issues related to the role of emerging powers in the global nuclear order, nuclear nonproliferation, nuclear security, strategic trade management, and proliferation financing controls.

TKassenova@ceip.org