TESTIMONY BEFORE THE HOUSE COMMITTEE ON FINANCIAL SERVICES SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

Countering the Financial Networks of Weapons of Proliferation

Tom Keatinge, Director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute

Introduction

Chairman Pearce, Ranking Member Perlmutter, and distinguished members of the Subcommittee, thank you for inviting me to testify today about strategies to disrupt the financing and procurement of weapons of mass destruction; and the role financial institutions (broadly defined) can play in identifying proliferation financing activities. Given my home base is London and the focus of RUSI's counter proliferation finance (CPF) research is on Southeast Asia and sub-Saharan Africa, my remarks will necessarily address to a greater extent the international CPF architecture, as promoted by bodies such as the United Nations and Financial Action Task Force (FATF), rather than the policies laid out by US domestic agencies. The US however, has a key role to play in strengthening this architecture, particularly as it takes on the Presidency of the FATF for the next 12 months.

Since 2015, thanks to the generous funding support of the John D and Catherine T MacArthur Foundation, RUSI has conducted extensive and wide-reaching research into the global counter-proliferation finance regime, assessing the awareness and effectiveness of governments and their private sectors in implementing proliferation finance controls.

Our research has produced four main papers as detailed below, all of which are freely available to governments and private sector actors:

- 2016: Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance
- 2017: Countering Proliferation Finance: An Introductory Guide for Financial Institutions
- 2017: Countering Proliferation Finance: Implementation Guide and Model Law for Governments
- 2018: Underwriting Proliferation: Sanctions Evasion, Proliferation Finance and the Insurance Industry

We have also conducted outreach and training presentations in a number of countries in Southeast Asia, Europe and Africa, working closely with key government and private sector stakeholders in those countries to strengthen national responses to the illicit financial networks of proliferators. This work will continue in 2018/2019.

Consistent with the focus of the hearing, this submission, primarily based on the above-referenced titles published by RUSI, will cover the following fields: a background to the CPF status quo; a review of currently assessed global CPF capabilities; observations on and recommendations for the role of

financial institutions in tackling proliferation; wider supply chain vulnerabilities; and recommendations for stakeholder action.

Background

In 2012, the Financial Action Task Force (FATF), the international organisation responsible for co-ordinating government actions to counter financial crime and in which the US plays a leading role, broadened its recommendations to include measures relating to countering the financing of WMD, their delivery vehicles, and related goods and activities. The move to include this subject alongside terrorist financing and money laundering was seen by many of FATF's member states as a vital next step.

Prior to 2012, national efforts to combat proliferation finance had been highly uneven, and in many cases non-existent, despite UN Security Council resolutions, including Resolution 1540 and country-specific regimes, that detailed actions to counter proliferation finance. Although most countries had procedures in place to detect and prevent the flow of goods related to illicit WMD programmes, they did not have similar procedures in place to stem the flow of funds used to facilitate this dangerous trade.

Thus, independent, international leadership was needed to create a standard for CPF that would hinder the ability of proliferators to access and exploit the financial system. The FATF seemed ideally placed to offer such leadership.

When we began our research at RUSI, nearly four years had passed since the FATF incorporated recommendations on CPF into its international standards. Yet, despite the focus brought to the issue of proliferation finance by the FATF, RUSI's extensive interviews with governments, regulators and financial institutions (FIs) revealed that many of the shortcomings of the pre-2012 CPF landscape persisted. Put simply, very little had been done to put into effect the intentions expressed by the FATF in 2012 when it added CPF to its priorities. Governmental interest in proliferation finance and related outreach to FIs was highly uneven between national jurisdictions, with many countries providing no guidance on CPF to their financial sectors at all. The wide spectrum of approaches resulted in mixed messages being passed down from governments and regulators to their FIs.

For their part, FIs within FATF jurisdictions appeared generally alert to their obligations to enforce targeted financial sanctions (TFS) against individuals and entities specified in UN Security Council resolutions. Yet they were often ignorant of the enabling role of finance for proliferation networks and thus the proliferation threat beyond those sanctioned entities; they demonstrated a poor understanding of the nature of proliferation as an activity distinct from general sanctions evasion by states such as Iran and North Korea.

FIs were therefore often unclear as to what, if anything, they were expected to do to address the issue of proliferation finance beyond implementing TFS, believing in many cases that the CPF objective was achieved purely by avoiding business related to Iran and North Korea.

The combination of mixed messages, unclear expectations and lack of guidance meant that unsurprisingly FIs were struggling to devise their own internal approaches to mitigate relevant risks.

This has resulted in proliferators, such as North Korea, being able to access and abuse the international financial system in support of their proliferation ambitions with relative ease. The nuclear ambition of a state such as North Korea requires both the procurement of material and the raising of funds to source the required goods and services, and access to the international financial system is key to carrying out these activities. It thus seems axiomatic that targeting the financial networks of proliferators should be a global response to such threats.

To-date, the international community has primarily addressed state-based proliferation activity via controlling certain goods and sanctioning bad actors. Yet this approach is fragmented, poorly enforced and too narrowly focused. As a cursory review of the UN North Korea Panel reports will reveal, proliferators such as North Korea employ an array of funding operations, such as repairing and servicing military equipment; training police forces; and building statues, and a range of commercial trading activities which involve both a logistical and financial operation. All of these activities generate money flows.

Thus, focusing merely on goods, either preventing their sale or interdicting their transfer once purchased, is just one part of establishing an effective response. Proliferators depend on access to financial assets and services, and the international financial system has become a critical lifeline for the regime. Detecting and stopping financial access will complicate and obstruct the wider operations of proliferation networks.

Reviewing Current International Capabilities

The FATF is currently undertaking a global evaluation of countries' compliance with its 40 Recommendations for combatting financial crime, and the effectiveness of such compliance.

As of mid-May, 50 countries have been reviewed in the current round, running since 2014 (the US review was published in December 2016).[1]

Two primary elements of the FATF's review address CPF:

- Recommendation 7 assesses whether countries have the necessary frameworks in place to 'implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing' and that such frameworks should ensure that countries can 'freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any

[1] United States, Mutual Evaluation Report (December 2016), available at http://www.fatf-gafi.org/countries/u-z/unitedstates/documents/mer-united-states-2016.html

person or entity designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations.'[2]

- Immediate Outcome 11 characterises an effective system as one in which 'Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) are identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for the financing of proliferation. Targeted financial sanctions are fully and properly implemented without delay; monitored for compliance and there is adequate co-operation and co-ordination between the relevant authorities to prevent sanctions from being evaded, and to develop and implement policies and activities to combat the financing of proliferation of WMD.'

Compliance with FATF Recommendations and Immediate Outcomes is assessed on a four-step scale from 'non-compliant' to 'compliant' and 'high' to 'low', respectively. The chart below, drawn from data provided by the FATF,[3] depicts the extent of assessed compliance and effectiveness for R7 and IO11 thus far.

	Recommendation 7 Compliance				**Immediate Outcome 11 Effectiveness**	
Compliant	8	16%		***High***	1	2%
Largely-	9	18%		***Substantial***	14	28%
Partially-	17	34%		***Moderate***	12	24%
Non-compliant	16	32%		***Low***	23	46%
Total	**50**	**100%**		**Total**	**50**	**100%**

USA rated Largely Compliant and High Effective in December 2016

As can be clearly seen, two-thirds of assessed countries are non- or only partially-compliant with the requirement to be able to impose TFS without delay; and 70% of assessed countries have a low or moderate level of effectiveness, meaning they suffer from major shortcomings.

It is clear that notwithstanding the prioritization of CPF in 2012, the global community still has considerable work to do to harden the financial system against abuse by proliferators.

It is important to note that compliance with FATF standards alone does not result in effective CPF controls. In fact, FATF's recommendations are now increasingly out of touch with other international obligations on CPF. UN sanctions against North Korea incorporate measures that go beyond list-based sanctions implementation, and focuses to a greater extent on activity-based obligations to counter proliferation finance. This includes requirements to restrict relationships with North Korean financial institutions and joint ventures. The recent FATF guidance published in March 2018 acknowledged this risk, stating that 'as list-based targeted financial sanctions alone cannot

[2] The FATF Recommendations, p11

[3] The Financial Action Task Force, *Consolidated Assessment Ratings* (18 May 2018), available at http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html

address illicit procurement and proliferation financing' implementation of UN measures that go beyond FATF requirements 'contributes to a stronger counter proliferation financing regime'.[4]

Furthermore, while the FATF requirement to implement targeted financial sanctions technically goes beyond those individuals and entities named on sanctions lists (to also include anyone owned by, controlled by or acting on behalf of or at the direction of those designated entities and individuals), this is not always reflected in implementation. It is RUSI's experience that countries and financial institutions focus on designated entities and individuals alone, and not their associated networks.

Securing the Financial System Against Abuse by Proliferators

Despite export control measures and international treaties seeking to prevent the further spread of nuclear, chemical and biological weapons and their related delivery systems, proliferators have been able to procure and acquire goods for these programmes with relative ease. International efforts to counter this have typically been devoted to the detection and seizure of physical goods, materials and technologies.

However, proliferation efforts rely also on finance to facilitate this illicit trade. Indeed, procurement of sensitive WMD-related goods is made possible by the international financial system. Reports from the UN Panel of Experts on North Korea, for example, have highlighted that Pyongyang is 'using greater ingenuity in accessing formal banking channels' to support illicit activities and WMD proliferation.[5] The most recent Panel report observes that North Korea 'continued to access the international financial system because of critical [sanctions] implementation deficiencies, which resulted in the country's evasive activities not being duly identified and prevented. The deceptive practices of the Democratic People's Republic of Korea and the lack of appropriate action by many Member States are systematically undermining the effectiveness of financial sanctions.'[6]

The role played by the financial sector in disrupting proliferation finance has received greater attention in recent years. Some governments maintain that financial institutions have both the capability to detect, and an obligation to disrupt, financial transactions in support of illicit WMD proliferation. However, government initiatives on countering proliferation finance vary widely between jurisdictions.

In addition to the research we have undertaken at RUSI to assess the capabilities of governments and their private sectors as relates to CPF, we also undertake training and provide technical assistance to these stakeholder groups – particular FIs who are placed on the frontline of

[4] FATF, 'FATF Guidance on Counter Proliferation Financing', March 2018, p. 15.
[5] UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017, p. 4.
[6] UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2018/171, 1 March 2018, p. 59.

implementation by their governments with limited support provided – to help equip them to better understand and mitigate proliferation financing risks.

This capacity-building activity reveals extensive gaps in knowledge, awareness and capabilities, and – perhaps more worryingly – highlights considerable misunderstanding with regards to the risks posed by proliferators, often conflating CPF activity with compliance with sanctions' regimes. We have found that while many FIs may have certain basic controls in place to counter proliferation finance, 'on the whole [they] do not understand the contemporary realities of the threat they are facing',[7] and are failing to implement adequate internal approaches to counter proliferation finance.

However, as outlined earlier, financial institutions have an important role to play in preventing proliferators from accessing the formal financial system and securing financial services in support of proliferation sensitive trade that goes beyond simply implementing targeted financial sanctions – as those on sanctions lists are unlikely to seek to transact in their own names.

It is therefore important that financial institutions take time to better understand and mitigate proliferation financing risk. Proliferators have become increasingly skilled at circumventing the sanctions imposed against them and gain access to the financial system through extensive networks of corporate entities (including front companies), middlemen and circuitous payment patterns.

In most cases, there will be no obvious paper connection to jurisdictions of proliferation concern. For financial institutions that have carried out little or no concerted thinking on this subject as distinct from other forms of financial crime, there are a number of approaches that can easily be adopted to improve the FIs contribution to CPF efforts. From our research at RUSI, we have identified three primary means by which the financial sector can support the hardening of the financial system against abuse by proliferators.

- First, situational awareness and education about the risk at hand: this includes conducting an internal risk assessment to better understand potential exposure to proliferation financing – as distinct from sanctions risk – and the areas of concern which would require mitigation. Few FIs interviewed by RUSI have made use of key information sources such as UN Panel reports and very few FIs identified a relevant staff member who tracked CPF associated publications from the FATF, UN or other government or academic bodies.

- Second, 'know your customer' (KYC) efforts should move beyond focusing merely on the entities and individuals listed on sanctions lists. Instead, FIs should familiarise themselves with the wider networks of proliferating actors. This includes ensuring that customer due diligence processes include the gathering of information that is relevant to proliferation financing, and not just other types of financial crime, and dedicating resources to conducting investigations into the networks of customers considered higher risk or operating in certain areas of the world, or sectors of the economy. While no approach to countering proliferation

[7] Emil Dall, Andrea Berger and Tom Keatinge., 'Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance', RUSI Whitehall Report, 3-16 (June 2016), p. 19.

finance is fool-proof, a few simple adjustments to internal policies can go a long way to ensuring that a financial institution has a baseline policy for dealing with proliferation financing risk and can help mitigate the risk of inadvertently being caught up in proliferation financing activity.

- Third, identifying proliferation sensitive goods and technology: whilst the first two actions are relatively straightforward for FIs, identifying the procurement and shipping of proliferation sensitive goods is highly challenging, and arguably impossible for a financial institution to achieve, absent the provision of intelligence leads. Still, FIs should familiarise themselves with export control regimes, and which clients fall under those controls. FIs should also, having educated themselves about the risk of proliferation finance as part of the two previous actions, be aware of any transactions that fall outside of usual business activity and fit proliferation finance patterns.

Whilst there are clearly considerable improvements that FIs can make in staff awareness and fine-tuning KYC checks and due diligence processes to reflect proliferation finance risk, the CPF effectiveness of financial institutions will be greatly enhanced by information and intelligence support provided by national governments and international organisations. In our research, we found very few cases where governments worked with FIs to enhance their CPF capabilities, even if they had established partnership mechanisms for engaging with FIs on other issues such as terrorist financing and human trafficking.

Vulnerabilities Across the Supply Chain

The need for governments to engage with the private sector is not limited to a narrow definition of the financial sector. As sectoral sanctions have been increasingly applied to North Korea, it has undertaken creative and deceptive activity to secure funding from the sale of coal; it has also undertaken at sea ship-to-ship transfers to secure the energy products it needs. These activities bring into scope other industries needed to secure the integrity of the international supply chain that would benefit from engagement with national governments such as shipping companies, commodity brokers and insurance companies, all of which lag the banking sector in terms of awareness of, capability and commitment to the global CPF agenda.

Whilst the banking sector must continually strive to improve its standards, it is not right that it should be the only element of the private sector that invests in capabilities to address the deceptive practices of proliferators. A 'whole-of-system' approach is needed in order to maximise disruption opportunities.

Conclusions and Recommendations

As evidenced by the FATF's evaluation data and the detailed reports of the UN Panel of Experts on North Korea, six years since the FATF introduced CPF as a third leg of focus alongside money laundering and terrorist financing, global CPF efforts are fragmented at best and ineffective/non-existent at worst.

Furthermore, the current FATF standards related to CPF are weak and simplistic:

- They do not require countries to assess their proliferation financing risks
- They focus merely on the implementation of targeted financial sanctions
- They are not risk-based in their application

In sum, the global architecture for disrupting proliferation finance requires improved design and implementation.

The following recommendations are therefore offered for the Subcommittee's consideration.

For the private sector

- Financial institutions must expand their awareness of proliferators' activities and ensure that CPF is an integral part of their financial crime compliance and investigations capability, with designated expertise.
- Other related private sector actors such as insurance companies, commodity brokers and shipping companies need to demonstrate greater commitment to disrupting the ambitions of proliferators, in particular North Korea.
- The private sector as a whole needs to develop methods of collaboration that create a joined-up, whole-of-system response, that hardens the supply chain to abuse by proliferators.

For international organisations such as the FATF

- Although the FATF has recently made a welcome update to its CPF guidance,[8] with certain notable exceptions (such as the work undertaken by the FATF-style regional body in Asia, the Asia Pacific Group on Money Laundering), work across the FATF network on CPF lacks prioritisation. The country assessments conducted since 2014 highlight serious, systemic failings that need to be urgently addressed.

For the US Government

- From July 2018, the US assumes the presidency of the FATF (led by the Treasury Department's Office of Terrorist Financing and Financial Crimes). CPF is a stated priority of the US Presidency of the FATF over the next 12 months.[9] The US should use this position not only to continue efforts to raise global standards in line with current requirements, but also to review the adequacy of current FATF standards in order to promote opportunities to strengthen and broaden the status quo.
- Weaknesses in the global financial system will be exploited by bad actors, including proliferators and those seeking to raise funds in support of proliferation activities. A

[8] The Financial Action Task Force (2018), *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, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html

[9] Outcomes FATF-MENAFATF Joint Plenary, 27-29 June 2018, available at http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-june-2018.html

continued, relentless focus on strengthening the integrity of the financial system, in its entirety, should be prioritised by the US Government.

For all national governments

- Financial institutions are placed on the frontline by the FATF, the UN and national governments. A failure by national governments to support the security role delegated to FIs results in material and systemic vulnerabilities. Establishing information exchange partnerships between governments and relevant private sector actors can greatly enhance the effectiveness of the role FIs are required to play.[10] The complexity of CPF for the private sector makes such partnerships critical to the development of an effective CPF response.

[10] For further details see Nick J Maxwell and David Artingstall (2017), The Role of Financial Information-Sharing Partnerships in the Disruption of Crime, RUSI Occasional Paper

Annex: Speaker and Organisation Details

Tom Keatinge, Director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute

This submission is prepared by Tom Keatinge, the Director of the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI). RUSI is a donor-funded London-based defence and security think-tank, founded in 1831, and is registered with the Charity Commission for England and Wales (registration number: 210639).

Founded in December 2014, the CFCS is dedicated to addressing the challenges and effects of financial/economic crime and threat finance to the UK and international security and the important role finance can play in identifying and disrupting a range of globally-recognised threats. The team includes expertise from banking, law enforcement and international policy bodies such as the Financial Action Task Force.

Prior to joining RUSI in 2014, Tom was an investment banker with J.P. Morgan in London and New York for 20 years.

He has a Masters in Intelligence and International Security from King's College London, completed in 2012 whilst on a one-year sabbatical from J.P. Morgan. His Masters research focused on the effectiveness of the global counter-terror finance regime.

He has a BA in Modern Languages from the University of Durham (1990-1994).