Project Alpha
Centre for Science and Security Studies
King's College London

KING'S College LONDON

Trade Finance and Proliferation Finance - Mitigating the Risks

Report on Workshop organized by Project Alpha at the Centre for Science and Security Studies, King's College London, on 20 June 2017

Background

Financing the proliferation of WMD is poorly understood and difficult to identify. Procurement networks hide their financial tracks to circumvent sanctions or other controls. Sources of funds, which may be countries under sanctions, are concealed behind front companies or individuals acting on their behalf. Goods and materials procured by proliferation networks are generally industrial in nature and usually obtained from established overseas, often via brokers. Financial transactions are typically processed through the international banking system and usually appear to be related to legitimate trade. They may take place on "open account" terms" or supported by trade finance operations.[1]

In this context, on June 20, 2017, the workshop "Trade Finance and Proliferation Finance – Mitigating the Risks," took place at King's College London, UK. The objective of this workshop was to examine what is known about how current mechanisms for financing global trade might be exploited for the purposes of financing of proliferation (FoP) of Weapons of Mass Destruction. The workshop took place in the context of a study carried out by Project Alpha, funded by United States Department of State, of current typologies of FoP. Participants included representatives from the commercial sector, amongst these banks, consultancy firms, insurance companies, and others, and the government sector, including the UK and US governments, and crown dependencies. The discussion took place under the Chatham House rule and was structured roughly into: challenges, regulatory expectations, possible solutions. The workshop aimed to 1) Review current mechanisms for trade finance and identify how these may be exploited for financing proliferation; 2) Identify possible measures governments and financial sector could take to mitigate risks; and 3) Consider mechanisms for information sharing to support risk mitigation. Topics discussed included the extent to which current risk assessments

[1] It is estimated that 80% of normal trade transactions take place on "open account" terms (The Wolfsberg Trade Finance Principles (2011)).

extend to FoP, the priority given to identifying FoP; trends in the relationship between FoP and trade finance, current red flags to identify FoP, methods to mitigate risks, comparisons of FoP between different proliferation programmes and sources of expertise.

The following report is a summary of main points and is not intended to be a comprehensive record. It is structured as follows: First, the main issues discussed during the workshop highlighted as the main challenges for the financial sector are described. Second, the specific options for mitigating risks are delineated. Finally, a list of recommendations and follow up action items have been compiled by the workshop organisers and based on the workshop discussions are noted.

The Problem

1. Lack of Understanding and Priority

FoP is rather poorly understood by most financial institutions. In addition, the risk of FoP is given low priority by most governments, including the UK government (it does not feature for example in the UK National Risk Assessment). Most law enforcement investigations of offences relating to proliferation focus on goods and materials, which are easier to identify and prosecute, rather than the related financing.

There is often little intelligence available to government departments relating specifically to FoP. Law enforcement departments rarely receive specific reporting. In most cases intelligence is too sensitive to be shared with the financial sector, and other potentially useful information, such as export license refusals, is not shared.

More generally, the potential role of trade finance in financial crime is better recognized. In the UK, the many ways to finance trade have been regulated by law since 2003. Some of the instruments governing trade finance are however of codes of practice rather than law.

Different banks have different approaches to addressing trade financing risks, depending on priorities and risk assessments. Their ability independently to identify FoP depends amongst other factors on the quality of information available to them through conduct of their business, including from trade-related documentation and SWIFT messages. A fundamental problem is

that trade documentation is not standardized, and there is no requirement for details of financing of goods covered.

The human element is also important. Compliance departments within financial institutions are often regarded as cost centres and junior employees may have insufficient training or authority to flag possible FoP related transactions.

Although the financial sector submits many Suspicious Activity Reports (SARS) they do not often refer specifically to FoP and may contain insufficient details, such as names of companies, to enable authorities to initiate investigations of FoP. Sometimes the information in SARs does not become useful until several years later, perhaps in support of investigations initiated by other triggers. Due to several factors, among them the sensitivity of information, information resulting from SARS is rarely relayed back to the financial sector.

2. Dual-Use Goods

Identifying dual-use goods is a challenge for the financial sector. There are many control lists from different sources and comparing lists with documentation available to banks may be difficult. There is no industry standard and some banks have created their own lists. This problem is compounded by the lack of clear guidance from regulators on the issue of dual-use goods: is dual-use goods screening required, and if so, against what lists and with what purpose? Due to the technical nature of the lists, financial institutions may need assistance in developing the know-how and understanding to integrate systematised risk assessment or red flag indicators related to dual-use goods into their screening procedures. Financial institutions also often differ in their definitions of key terms.

E-commerce carries significant risks of financial crime in general and FoP in particular. Many sensitive proliferation-related components can be purchased over the internet. Dual-use items are traded on open market places and may not leave a paper trail, creating the risk that financial institutions become unwitting participants.

Mitigating the Risks

1. Risk Assessments

Governments ideally should set an example for their financial sectors by incorporating FoP risks into their National Risk Assessments. Doing so would be consistent with the thrust of Financial Action Task Force (FATF) Recommendation 1 (even though as drafted Recommendation 1 makes no reference to FoP). Governments should also ensure that departmental responsibilities are appropriately clear to prevent the issue of proliferation finance 'falling between the gaps'. It is important to identify which government department should lead on this issue to ensure that it is adequately addressed.

Depending on their business model, different financial institutions will have different exposure to FoP. But a formal FoP risk assessment, and subsequent action dependent on the outcome, would constitute good practice.

2. Red Flags

The basic lists of red flags for FoP were published by the FATF in 2008,[2] and these have been added to by other institutions. However, published FoP red flags are not in many cases uniquely diagnostic and it is not clear to what extent specific red flags are incorporated into financial institutions' transaction monitoring systems. Often compliance specialists make judgments on other bases when checking trade-related financial transactions.

One of the objectives of the Alpha Project's typologies project is to try to refine the currently available lists of red flags.

3. Know Your Customer (KYC) and Monitoring

Monitoring customers' business profiles and patterns of financial transactions are a central element of due diligence conducted by financial institutions, and in the absence of other detailed indicators that could be checked, such as invoices or detailed bills of lading or other shipping documents, is an important potential element in identifying FoP.

[2] FATF Typologies Report on Proliferation Financing, 2008 (http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html)

4. Goods Screening

Many different government dual-use control lists are available, and big data analytics can be used for different purposes by research and financial institutions. King's College London produces reports using open source intelligence and has recently launched Alpha-POST, an open source information-collation tool that includes a capability to screen transactions against lists of dual-use goods keywords. There is room to explore potential synergies in the field of research and education.

5. Information Sharing

Better systems to share information, and a common understanding of what information could most usefully be shared, is vital to combating FoP. Better information sharing of experiences and typologies of FoP between financial institutions is important. Many government-private partnerships already exist for information-sharing on trade finance. These partnerships contribute to more effective reporting and enforcement of financial crime. Some examples presented include JMLIT, the Hong Kong Fraud and Money Laundering Intelligence Task Force, the U.S. Anti-Money Laundering and Counter-terrorism Consortium, the Singapore Anti-Monday Laundering and Countering the Financing of Terrorism Industry Partnership, and the Australian Fintel Alliance. The best way to bridge many of the information gaps relating to FoP in the UK would be to incorporate FoP into the formal JMLIT agenda.

It was noted also that there are datasets available on entities of proliferation concern, among other issues, and that these could be made available to the financial sector to assist in compliance and KYC activities. KCL is examining practical ways of making its datasets more systematically available to the financial services sector.

6. Setting Industry Standards

Banks have a potentially important role to play by identifying and publicising standards of practise to combat FoP that they implement, and that they require business partners to implement. Ultimately, however, the responsibilities of the financial services sector must be in line with the requirements of regulators, and it is for regulators to set high standards of requirements and expectations for FoP. While it is recognised that governments might be hesitant to set specific standards, regulators and financial sector should work together to address questions such as "is dual use screening required" and" how much is enough?".

7. Culture/Capacity-Building

Middle and low-level employees in relevant departments of financial institutions are key players in identifying FoP. Providing opportunities to educate them at least to a basic awareness level is important. E-learning or short courses could be considered. Education is also important to clarify and place into context the issue of dual-use control lists and their use in screening.

The training offered by the UK Export Control Organisation (ECO) was highlighted as being potentially useful. However, it was also noted that the ECO's training was not well suited to the financial services sector as the ECO does not believe that financing of proliferation falls within its mandate. With this in mind, KCL undertook to explore the provision of a dedicated course on aspects of the problem, including dual-use goods identification, perhaps in partnership with a government department.

Capacity-building is also important on the international level. Outreach programmes, such as the United States Department of State's Export Control and Related Border Security Programme, invest resources into developing the export control systems of countries, and raising awareness, and providing expertise and training on FoP.

8. SARs/STRs

There is a need to look at ways to improve quality of reports. Including requiring more detail in SARs/STRs (such as names of companies involved), and specifically identifying FoP, will enable authorities better to identify and investigate FoP and thus the underlying procurement networks. A possible model is 'Project Brass', a now-defunct government initiative under which reporting parties were instructed to include the term 'Brass' in any SAR that they believed was related to financing of proliferation.

9. Vessel Tracking

Commercial vessel tracking systems, such as the Automatic Identification System (AIS), enable both real-time and historical checks on vessel movements, and thus determinations of possible travel or port calls connected with proliferation and FoP. Commercial services are also available to screen beneficial owners and other parties related to the vessel. The role of such tools in

managing risk was highlighted as important by some participants, even if the regulatory requirement for their use is somewhat unclear.

Recommendations

The following are based on the views of the organisers:

1. JMLIT should include FoP risk and its mitigation into its agenda;
2. Suspicious Activity Reports/Suspicious Transaction Reports should refer specifically to FoP where this is believed the case, and include more detailed FoP information;
3. National Risk Assessments and other Risk Assessments should cover FoP risk;
4. Governments should look at ways to provide better information and feedback to financial sector relating to FoP;
5. Financial institutions should integrate capacity-building and education on FoP into training for staff;
6. Regulators should set clear responsibilities for financial institutions relating to FoP;
7. Institutions should set high industry standards on FoP for business partners;
8. Governments should consider revisiting Project BRASS.

The organisers will follow up.