Financial institutions and the threat of proliferation finance

Proliferation finance is a topic and issue that provides significant complexities for companies seeking to manage the associated risks. For Financial Institutions there has never been a more important time to tackle this issue, and recently the Financial Action Task Force have updated their guidance on proliferation finance. **Dr Jonathan Brewer** sets out the background of proliferation finance and explores some of the ways Financial Institutions and their customers can identify the risks, allowing them to understand mitigate them.

For years, national authorities have regarded proliferation finance ('PF') as less of a threat to the integrity of the global financial system than money laundering ('ML') or terrorism financing ('TF'). This attitude is changing: The threat from proliferation of weapons of mass destruction ('WMD') to international peace and security, and thus financial stability, is arguably as least as great, or greater, than ML or TF, and controls on PF are an important element of international efforts to counter such proliferation. Three or four years ago providers and funders of PF training courses had to knock on doors to get people to look at PF seriously. Demand for PF training now is much higher.

Pressure on authorities and the financial sector to implement PF measures is about to increase significantly. In October 2020, the Financial Action Task Force ('FATF') modified its Recommendation 1 to include PF in the existing requirement to carry risk assessments for TF and ML.[1] The US Department of Treasury has also included PF amongst government-wide priorities for ML and TF.[2] These represent big steps forward on PF by the international financial community.

Most financial institutions and designated non-financial businesses and professions (hereafter referred to as 'FI's) have tried to meet PF challenges by complying with sanctions, and some have relied also on existing programmes to monitor and control ML or TF. They will now need to do more on PF, but help is available. In addition to publications by FATF, several academic institutions and think tanks have issued reports on PF typologies and risk assessments, and an increasing number of training courses are on offer.[3] FI staff can take well-informed actions to protect your institution ('PYI') and to promote international peace and security ('PIPS').

Overview

International controls on PF originate in United Nations Security Council ('UNSC') Resolutions. These include Resolution 1540 (2004) focused on non-State actors, and country-specific sanctions: Resolution 2231 (2015) relating to the Iran nuclear issue, and Resolution 1718 (2006) and successor sanctions resolutions relating to DPRK's WMD programmes. In response, FATF published a PF typologies report in 2008,[4] and FATF's international standards of 2012 included a requirement (Recommendation 7) to comply with UNSC targeted financial sanctions ('TFS'), and the freezing of associated assets.[5] FATF modified this rules-based approach to PF in October 2020 by extending the scope of its Recommendation 1 to include PF-related TFS risk assessments, in addition to ML and TF risk assessments.[6] This new requirement, on countries and FIs, will almost certainly improve implementation of UNSC TFS even though the UNSC Resolutions ('UNSCR') themselves do not require PF risk assessments.

This said, additional UNSC controls on PF, such as activity-based sanctions and sectoral sanctions are not included in FATF Standards. FATF published comprehensive PF guidance in 2018 on these additional UNSC PF controls but it is non-binding.[7] Implementation of these other categories of PF controls remains weak globally, and regulatory requirements regarding PF in general uneven. Few jurisdictions criminalise PF, for example, and few countries have conducted PF risk assessments. Weakly regulated jurisdictions are at greater risk of exploitation by proliferators.

Furthermore, few countries have published guidance for their private sector. Most FIs regard PF as a sanctions compliance challenge and few FIs incorporate PF indicators into existing programmes to monitor and control ML or

TF. Few FIs submit reports on PF to their regulators, thus potentially depriving national authorities of information useful for national PF risk assessments. Furthermore, restrictions on data sharing between FIs, and between authorities and FIs, may prevent information exchanges needed to identify a complete PF network. Such networks may have global reach and individual FIs may be involved in, and 'see', only parts of them.

FATF Mutual Evaluation Reports ('MERs') are important for shaping perceptions of the cleanliness of a country's financial system. To date, however, relatively few countries have scored well on Recommendation 7,[8] but the need to improve has encouraged several to organise workshops or meetings with PF Experts.[9]

How well countries meet the new PF requirements of Recommendation 1 will be assessed by FATF during the next, fifth round of MERs. The outcomes could result in a significant increase of knowledge and understanding of the scale and nature of the PF threat globally.

What is WMD proliferation finance?

State-sponsored WMD programmes involve activities ranging from in-country (domestic) research and development, manufacture and possibly testing, to overseas procurement of materials, equipment and technology, as shown in Figure 1. Figure 1 also illustrates the areas where non-State actors might also be working either in support of such programmes (on a commercial basis, in the form of trading companies, brokers, manufacturers, freight forwarders, financiers and other types of businesses and businessmen), or developing their own programmes (terrorists, for example), or in the form of criminal networks procuring or smuggling related goods, materials or technology.

> "MOST FIs REGARD PF AS A SANCTIONS COMPLIANCE CHALLENGE AND FEW FIs INCORPORATE PF INDICATORS INTO EXISTING PROGRAMMES TO MONITOR AND CONTROL ML OR TF.

WMD proliferation programmes need to be paid for, and listed in Figure 1 are activities included in a provisional definition of PF published by FATF in 2010.[10] These fall into two main areas: in-country development and manufacture of WMD (on the left-hand side), probably largely financed or funded in the case of State programmes by State budgets (probably with the involvement mainly of domestic FIs) and; activities related to procurement of goods and materials to feed these programmes, from source countries overseas (right-hand side). The channels to ship goods and materials from overseas are usually different from the related funding/financing channels.

If sanctions are in place (as in the case of DPRK and as illustrated in Figure 1), communications between these two areas of activity are probably significantly disrupted. If, however, there are no sanctions (as in the case of Pakistan's or India's WMD programmes) other barriers to overseas procurement may exist in the form of national export controls implemented by source countries overseas.

FATF's 2010 provisional definition of PF does not include fundraising activities. However, apparently in accordance with the proposition that '[a]ny revenue that North Korea generates can be used to support, directly or indirectly, its weapons development programs'[11] a number of UNSCRs since 2016 have targeted DPRK's fundraising activities, including sales of statues (UNSCR 2321 (2016)), sales of seafood, coal, minerals and products of other economic sectors (2371 (2017)), and prohibitions on DPRK workers earning income abroad (2397 (2017)). As a result, the definition of PF has in practice extended to fundraising activities.[12] This is unfortunate typologies and case studies relating to DPRK trade in seafood, coal or other minerals are unlikely to be the same as those related to fundraising by other State-sponsored WMD programmes. By contrast, typologies and case studies relating to 'pure' PF as defined by FATF in 2010, if incorporated into existing procedures to monitor and control ML or TF, could in principle enable FIs to identify not only transactions relating to existing WMD programmes, but possibly also relating to nascent or future programmes.

What is the global scale of the PF threat?

Little information is available to make an accurate determination of scale, although a number of indicators exist. For example, a shipment of industrial goods of WMD proliferation concern might cost hundreds of thousands of dollars, but given the relatively small number of WMD programmes globally such shipments in themselves are unlikely to represent a threat to the integrity of a jurisdiction's financial system. However, most international trade is conducted in US dollars and some estimates can be made of the impact of PF on the US. In designating the DPRK as a jurisdiction of primary money laundering concern in 2016 under Section 311 of the USA Patriot Act, the US Treasury's Financial Crimes Enforcement Network (FinCEN) noted that 'deceptive practices have allowed millions of US dollars of DPRK illicit activity to flow through US correspondent accounts'.[13]

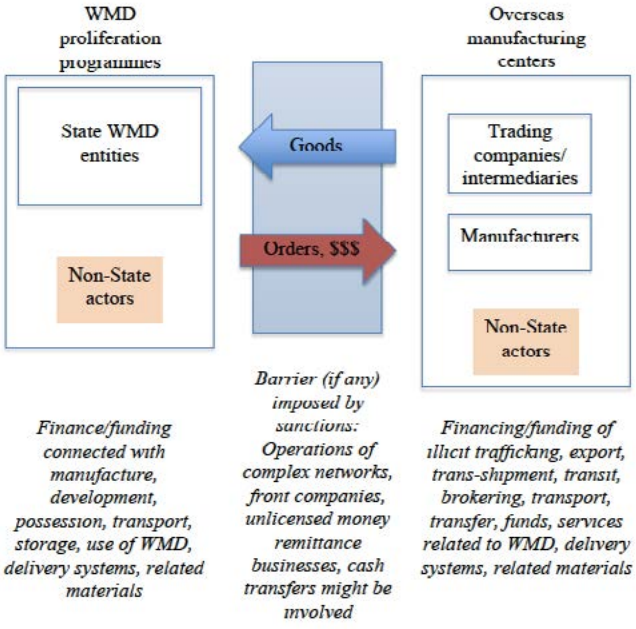

Figure 1: Schematic diagram of typical WMD programme activities, including possible state-sponsored and non-state actor elements. In italics, the related financing and funding elements.

> DECEPTIVE PRACTICES HAVE ALLOWED MILLIONS OF US DOLLARS OF DPRK ILLICIT ACTIVITY TO FLOW THROUGH US CORRESPONDENT ACCOUNTS.

Another US indicator can be found in enforcement cases reported by the US Department of Justice between the period January 2015 – January 2018. Based on the information supplied, perhaps 10% of these cases related to proliferation of WMD goods and materials and would thus have involved some aspect of PF.[14]

A case study of current PF networks

PF procurement networks, i.e., those that operate on the right-hand side of Figure 1, can be complex and globally extensive. Investigations by the Customs Administration of the Netherlands into one such network highlights details common to many cases of PF.[15]

In 2012, Dutch authorities received an export declaration from a Dutch company for a shipment, described as 'equipment for glass production', to a company in Tehran, Iran: Company A. The company, a wholesaler trading ferrometals, was owned by an Iranian living in Germany. The shipment was found to comprise 22 turbo vacuum molecular pumps that had been manufactured and supplied by a company in a second EU State. Under EU regulations at the time, a licence was needed for export because the pumps were considered to be of potential use in Iran's nuclear program. But the Dutch company had not attempted to obtain such a licence.

Further investigations by the authorities showed that, although on paper the Dutch company appeared to carry out a lot of business, in fact little of this was substantive and the company appeared to have no other business in the Netherlands. The authorities also found a number of fake invoices.

Although the documentation accompanying the intercepted shipment showed that the consignee of the pumps was Company A in Tehran, the Dutch company had told the supplier in the second EU State that they were destined for a new glass company in Turkey. Furthermore, a second company in Tehran, Company B, asked the Dutch company by email to change the name of the consignee from Company B to Company A. The investigators determined that Company B was a front company for the Iranian nuclear programme.

The Dutch Customs investigations also revealed that the Dutch company had received five payments by wire transfer into an account at a local Dutch bank from five different companies, based overseas, during a four-month period in 2011. Investigations showed that not all the five companies had a website. The Dutch company also had never applied for a license to receive these payments as required by EU regulations at the time.[16] The bank had no record of other transactions involving the five overseas companies.

The Dutch company paid the supplier of the vacuum pumps, in the second EU state, in instalments. The schedule of payments received and made by the Dutch company in this connection is shown in the Table below.

Although the total cost of the pumps was €232,500, a total of about €239,800 was paid into the Dutch company's banks account, suggesting that the company made a profit of about €7,300 on the deal.

Date	Payments received by the Dutch company from companies (all different) in:	Amount (€)	Description attached to payment	Action by trading company
March 2011	Turkey	36,185.00	Invoice No…	
March 2011				Payment to supplier
11 April 2011	UAE	44,926.00	Business transaction	
14 April 2011	Turkey	25,000.00		
14 April 2011	Jordan	55,480.00	Purchase	
15 April 2011				Payment to supplier
2 June 2011	Turkey	68,220.00	Based on First Glass	
12 July 2011				Payment to supplier
May 2012				Attempted export of vacuum pumps

Figure 2: Transactions related to the Dutch company's procurement of turbo molecular vacuum pumps, for shipment to Iran.

This case contains a number of features which have been seen in other cases of PF, including:

- Involvement of dual nationals; involvement of a small trading company; a company appearing to do little genuine business.
- Persistence: although the company had previously come to the attention of the Dutch authorities, it continued attempting to export goods without a licence.
- Unusual patterns of financial transactions: The large payments through the Dutch company's bank account in connection with the purchase of the pumps were not consistent with the company's normal business.
- Payments, received from different companies based in different countries, that together enabled the supplier of the pumps to be paid.
- Payments accompanied by vague and generalised descriptions of their purpose.
- Involvement of companies with no website.
- Transactions involving countries of diversion concern. Turkey and UAE are known to be countries through which goods or finances may be channeled in order to circumvent sanctions.
- An apparent consignee of a proliferation-sensitive shipment acting on behalf of a front company of a programme of proliferation concern.

PF in the future

Although the PF transactions identified in the Dutch case took place in 2011, the evidence from more recent cases of PF suggest that most typologies have not fundamentally changed over the last ten years. While the methods continue to work, proliferators will probably continue to use them. This said, according to reports of the UN Panel on DPRK, North Korean proliferation financiers are making increasing use of cyberattacks to raise funds. The Panel noted in August 2019 that total proceeds from

> "THE PANEL NOTED IN AUGUST 2019 THAT TOTAL PROCEEDS FROM DPRK-RELATED CYBERATTACKS ON FIS AND VIRTUAL ASSET SERVICE PROVIDERS ('VASP'S) WERE ESTIMATED AT UP TO $2 BILLION.

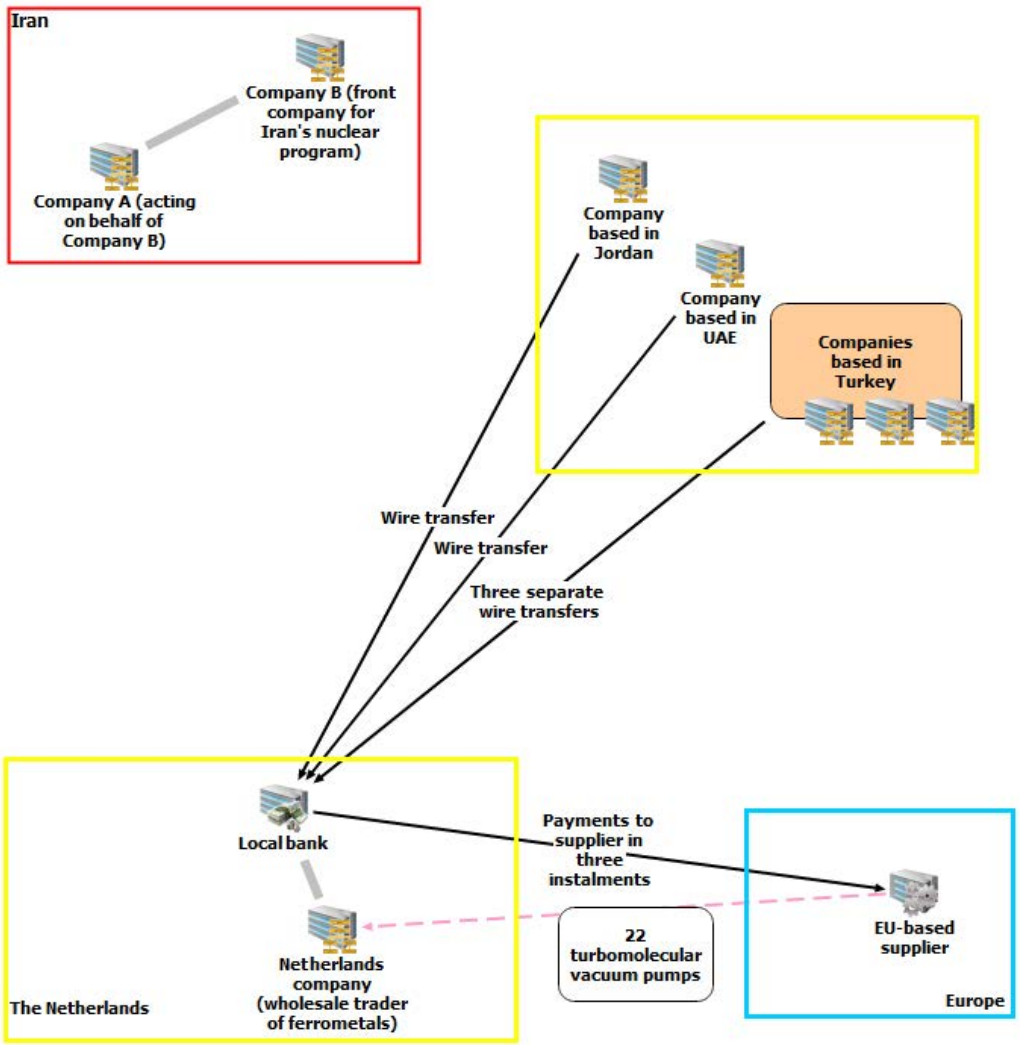

Figure 3: Schematic diagram to illustrate the relationship and financial transactions between entities involved in the Dutch company's procurement of vacuum pumps and their attempted shipment to Company A in Iran. See footnote 15.

DPRK-related cyberattacks on FIs and virtual asset service providers ('VASP's) were estimated at up to $2 billion, and in March 2021 the Panel noted that a UN Member State had valued the total theft of virtual assets by the North Koreans at approximately $316.4 million from 2019 to November 2020.[17]

To date there is no publicly available information that DPRK is using such stolen virtual assets specifically for PF, although if such assets were converted to a 'fiat' currency this would seem likely. And if, in the future, cryptocurrencies are used in international trade, it seems likely that DPRK would use them for PF purposes, for example to pay for procurement of goods and materials for its WMD programmes sourced from overseas.

Given their rapid evolution, it is likely that cryptocurrencies will become an important PF typology of WMD programmes in general. FATF to a certain extent has 'future-proofed' PF risks in this respect because virtual assets and VASPs need to be included in the risk assessments conducted by

States and FIs under FATF's Recommendation 1.[18]

How should FIs respond to the threat of PF?

FI staff responsible for mitigating PF risk should, ideally, focus on two objectives. The first is the need to protect your institution ('PYI') and the second, the need to promote international peace and security ('PIPS').

The Dutch case described above is an example of PIPS. Information about financial transactions obtained from a bank during the course of an investigation contributed to the authorities' ability to identify, in retrospect, the way this particular proliferation network operated. However, cases also exist of information provided by FIs (in the form of Suspicious Transaction or Activity Reports) that prompted authorities to pro-actively investigate proliferation networks.[19] To promote PIPS, therefore, FIs should have a PF policy in place to submit reports to regulators and law enforcement on PF or suspected PF where possible; to cooperate with law enforcement, including for example correlating law enforcement information with the FI database and providing feedback; and, where possible, to share PF information with other FIs.

FATF's modification to Recommendation 1 means that FIs will no longer be able to rely solely on rules-based sanctions screening to deal with PF, but will also need to implement a risk-based approach. In order to implement PYI effectively, therefore, FI staff will need to be educated about PF – not in order to turn bankers into WMD specialists, but to ensure they are alert to the

Dr Jonathan Brewer is a Visiting Professor at King's College London. From 2010 to 2015 he was the financial expert on the UN Panel of Experts for Iran, created pursuant to resolution 1929 (2010). Prior to this he was a member of Her Majesty's Diplomatic Service, serving from 1983-2010 his postings included the British Embassies in Luanda, Mexico City and Moscow. He holds a PhD in geophysics from Cornell University, New York, USA (1981) and a BA in Geology from the University of Oxford (1977).

Links and notes

1 Fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html

2 Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, Financial Crimes Enforcement Network, U.S. Department of the Treasury, 30 June 2021.

3 Examples of publications include: Proliferation Networks and Financing, Bruno Gruselle, Fondation pour la Recherche Stratégique, 3 March 2007; Emil Dall, Tom Keatinge, and Andrea Berger, Countering Proliferation Finance: An Introductory Guide for Financial Institutions, Royal United Services Institute (RUSI) Guidance Paper, April 2017; Jonathan Brewer Study of Typologies of Financing of WMD Proliferation Final Report, King's College London Project Alpha, 13 October 2017; Jonathan Brewer, The Financing of WMD Proliferation Conducting Risk Assessments, Center for New American Security, November 2018; Anagha Joshi, Emil Dall and Darya Dolzikova, Guide to Conducting a National Proliferation Financing Risk Assessment, RUSI, May 2019. Amongst other organisations, the US Department of State EXBS Programme and the UN Office on Drugs and Crime have funded or organised PF training courses.

4 FATF Typologies Report on Proliferation Financing 18 June 2008

5 FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, Updated October 2020

6 For these purposes, the FATF definition of PF risk is the 'potential breach, non-implementation or evasion of the targeted financial sanctions related to proliferation financing, as contained in FATF Recommendation 7'

This is a missed opportunity: a wider definition of PF could have aligned FATF's requirements more closely with PF requirements of UNSC resolutions.

7 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, 28 February 2018

8 A table of MER scores for individual countries can be found on the FATF website (www.fatf-gafi.org/ publications/mutual evaluations//documents/assessment-ratings.html)

9 For example, Latvia in May 2019 (www.mfa.gov.lv/en/news/latest-news/63568-riga-hosts-an-international-conference-on-compliance-with-sanctions-in-the field-of-proliferation-financing); Chile in October 2019 (www.uaf.cl/prensa/archivo_det.aspx?id+539)

10 This definition states that PF is 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 nonlegitimate purposes), in contravention of national laws or, where applicable, international obligations (Combating Proliferation Financing – A Status Report on Policy Development and Consultation, FATF, February 2010).

11 Testimony of Sigal Mandelker, Under Secretary, Terrorism and Financial Intelligence US Department of the Treasury Senate Banking Committee Thursday, 28 September 2017)

12 FATF Guidance on Proliferation Financing Risk Assessment and Mitigation, 29 June 2021.

13 Finding That the Democratic People's Republic of Korea Is a Jurisdiction of Primary Money Laundering Concern

A Notice by the Financial Crimes Enforcement Network, 2 June 2016)

14 Summary of Major US Export Enforcement, Economic Espionage, and Sanctions-related Criminal Cases (January 2015 to the present: updated 19 January 2018)

15 See Case 26 of the Study of Typologies of Financing of WMD Proliferation Final Report, King's College London, 13 October 2017

16 EU Regulations (961/2010) in force at the time required a license for financial transactions involving Iran larger that EUR 40,000, so the company should have applied for a license for three of the five payments and notified the authorities of the other two payments.

17 Report of 30 August 2019 (Security Council document S/2019/691) and Report of 4 March 2021 (Security Council document S/2021/211)

18 Interpretive Note to FATF Recommendation 15 on New Technologies (https://www.fatf-gafi.org/media/fatf/ documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf)

19 See for example Cases 17 and 22 of the Study of Typologies of WMD Proliferation Final Report, King's College London, 13 October 2017.

20 For further information see references in footnotes 1, 7 and 12.

21 Even where documentation is available however, the presence of proliferation-sensitive goods and materials may be difficult to establish, e.g How Does Global Trade and Receivables Finance Mitigate against Proliferation Financing? International Chamber of Commerce Document No.470/1284, 6 June 2019.

22 See paragraph 6.1 of The Wolfsberg Group, ICC and BAFT Trade Finance Principles, 2019 Amendment

23 See for example the Study of Typologies of Financing of WMD Proliferation Final Report, King's College London, 13 October 2017; 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, 28 February 2018

risk, know where to go for specialist advice if necessary, and can conduct a PF risk assessment.[20]

If FIs are involved in trade finance they may have access to documentation (letters of credit, invoices, bills of lading, customs documentation including HS Codes, etc) which can be checked for PF indicators.[21] However, the majority (perhaps 80%) of international trade takes place on open account terms,[22] and the related financial transactions (covered by SWIFT MT103 messages) provide little information on the nature of the underlying business. In this case, transaction analysis, based on incorporation of PF indicators into existing programmes to monitor for ML and TF, will be important.

FIs dealing with local banks located in countries with domestic WMD programmes (on the left-hand side of Figure 1) will need to establish an appropriate policy to mitigate the risk of involvement with PF.

Finally, a number of lists of PF indicators have been published.[23] These need to be tested and refined in order to optimise them for incorporation into existing FI monitoring systems. Perhaps an FI would make a database available to researchers for this purpose?

Conclusion

FATF's inclusion of PF into Recommendation 1, although focused only on TF, will prompt national authorities to conduct PF risk assessments and to require FIs to do so as well. Much new information about PF risk globally is likely to become available during the next round of FATF MERs.

This information will not only assist FIs to conduct their own risk assessments (thus promoting DYI), but should also serve as a focus for support to national authorities (PIPS).

Acknowledgements

This article benefited from comments provided by Jean-Annet de Saint-Rapt of the Centre for Science and Security Studies, King's College London. Any errors or misinterpretations are the sole responsibility of the author.