



## **Study of the Typologies of the Financing of Proliferation of WMD**

The proliferation of weapons of mass destruction (WMD) is a major threat to global peace and security. Detecting the financing of proliferation (FoP) can assist in combating WMD, but it is difficult and requires a better understanding of typologies. Typologies can assist governments in implementing sanctions on WMD programs and disrupting proliferation networks. They can also help the private sector to identify information that should be passed to governments, and to remain compliant with sanctions.

The most recent comprehensive review of FoP typologies is dated 2008<sup>1</sup>. Since then, more information on the financing of proliferation has become available, particularly relating to UN sanctions on Iran and on North Korea. Some of this information was published by the UN Sanctions Panel on Iran and is attached at Annex 1.<sup>2</sup> The examples relate specifically to Iran and illustrate both financing of proliferation and circumvention of financial sanctions.

The King's College Study is a year-long project funded by The Export Control and Related Border Security (EXBS) Program of the US Department of State. It's purpose is to gather and analyse information held by governments and by the private sector relating to both financing of WMD proliferation globally and

---

<sup>1</sup> Typologies Report on Proliferation Financing, 2008, Financial Action Task Force.

<sup>2</sup> Taken from reports published in June 2014 and June 2015 and available on the UN website ([www.un.org](http://www.un.org)), S/2014/294 and S/2015/401.

circumvention of financial sanctions, and to publish the results in the form of reports.

Analysis of information gathered from governments and the private sector will provide a better understanding of patterns, choice of financial sectors (both formal and informal) and channels characteristic of financing of different WMD proliferation networks (North Korea, Iran, others) and circumvention of financial sanctions, profiles of front companies and individuals involved, and trends and future developments.

Reports will be published consisting of case studies, risk indicators and typologies relating to financing of WMD proliferation globally and circumvention of financial sanctions. These will assist practitioners in governments to identify FoP or circumvention of financial sanctions and investigate individuals and entities involved, to disrupt proliferation networks, and to provide guidance to financial institutions regarding FoP and implementation of financial sanctions.

The reports will also assist banks, financial institutions and commercial concerns to remain compliant with sanctions and to identify transactions relating to FoP globally or circumvention of financial sanctions, and file a suspicious activity report or otherwise inform relevant government authorities.

Much of the relevant data held by governments will be classified, and data held by banks, financial institutions or commercial organisations may be governed by banking secrecy regulations or other restrictions. The study is not seeking the details of such data. It needs instead anonymised case studies, results of investigations, analyses, or other information that enables identification of patterns or trends of FoP. All information collected by the Project will be held in accordance with King's College London standards on security and ethics. Information in published reports will be anonymised.

For further information or to support the Study, please contact Dr Jonathan Brewer or Ian Stewart. Jonathan Brewer is a Visiting Professor at King's College, London (see bio at Annex 2). He can be contacted on +1 917 900 7636 (mob), on +44 7815 848 418 (mob), and on [Jonathan.Brewer@kcl.ac.uk](mailto:Jonathan.Brewer@kcl.ac.uk). Mr Ian Stewart is a Senior Researcher in the Department of War Studies at King's College London, and Head

of Project Alpha on Non-Proliferation. He can be reached on +44 207 848 1342 (off) and at [Ian.Stewart@kcl.ac.uk](mailto:Ian.Stewart@kcl.ac.uk).

Project Alpha  
Centre for Science and Security Studies  
Department of War Studies  
King's College London  
Strand  
London WC2R 2LS

October 2016

## **Annex 1**

The following examples were provided to the UN Sanctions Panel on Iran by governments and the private sector and published on the UN website (Reports of June 2014, S/2014/394, and June 2015, S/2015/401). They relate specifically to Iran but the King's College Study will extend to proliferation globally.

- A national authority described an example of a transaction involving intermediaries in multiple countries (see diagram below). The methods of concealment of the involvement of designated entities are to be noted: A purchase order was placed by a designated entity, Atomic Energy Organisation of Iran<sup>3</sup>). The purchase order was forwarded through a front company. Payment was initiated by a second front company in Iran through another designated entity, Bank Sepah<sup>4</sup> which transferred funds through an Iranian company in the food business to a non-UN sanctioned Iranian bank. From there, the transfer was made via a bank in the country A to a bank in country B.

---

<sup>3</sup> Listed on 23 December 2006 in Annex A of resolution 1737 (2006) (IRe.006).

<sup>4</sup> Listed on 24 March 2007 in Annex I of resolution 1747 (2007) (IRe.007).

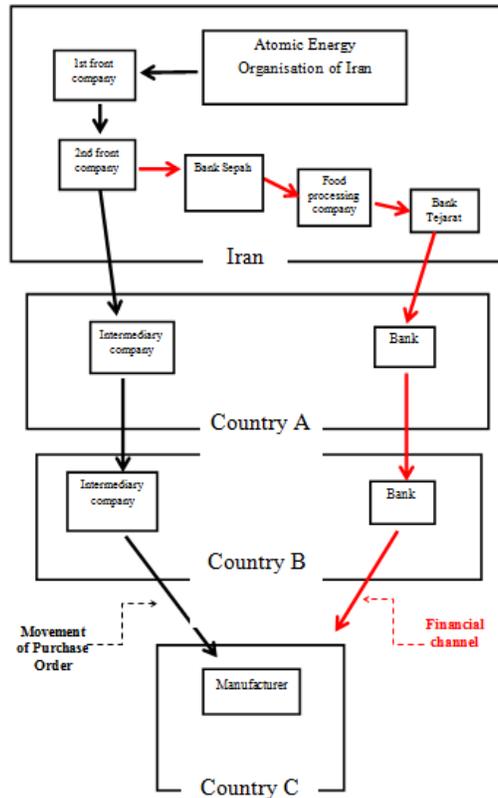


Diagram: A transaction scheme involving intermediaries in multiple countries

- A foreign national set up a trading company in a State in the Middle East and opened a series of accounts on behalf of the company at an international bank in the State concerned. These accounts were denominated in local currency and in euros, United States dollars, and other foreign currencies. Monitoring by the bank showed that the trading company's account received funds in local currency from only one source (a second company set up by another foreigner). These local currency funds were then quickly switched into foreign currencies and transferred overseas. This activity triggered investigations by the bank, which indicated that the owners of the companies involved had links to Iran. The bank suspected the funds were coming from Iran and being channeled through the trading company into the global financial system.
- A foreign national set up a trading company in a State in the Middle East and opened an account on behalf of the company at an international bank in the State concerned. Monitoring by the bank showed a high turnover of funds, and money-laundering was suspected. Investigations by the bank

showed that the foreign national's stated employment was as a member of staff in a second company, which had the same telephone number as the trading company. Further investigation revealed that this telephone number was the same as that belonging to two other companies previously identified by the bank as having Iranian shareholders and involved in Iranian business. The bank therefore suspected the trading company was being used as a front for Iranian business.

- A national of a State in the Middle East set up a company in that State in partnership with a foreign national as a minority shareholder, and opened an account on behalf of the company at an international bank in the State concerned. Multiple large payments were made from this account to several companies at the same address in a European country, and also to a second set of companies sharing an address in a second European country. The bank's monitoring identified this pattern as possible money-laundering, and further investigation revealed that the national of the State in the Middle East was also a manager of another company that did business with Iran.
- A payment for freight charges which named two logistic companies but which made no reference to Iran: at the request of the financial institution, an invoice was provided. This was found to contain a bill of lading reference number. Upon tracking this bill of lading, the final destination of the shipment was found to be Iran.
- A payment to a company in a State neighbouring Iran: the policy of the financial institution was to conduct enhanced due diligence where companies in this particular State were concerned and, as a result, this company (the beneficiary of the payment) was found to be located in Iran. The address in the neighbouring State was a fake.
- An import Letter of Credit (LC) covering a shipment of goods: the goods originated in State A in South Asia, ostensibly to be shipped from State B neighbouring Iran to State C in North Africa. The financial institution investigated the LC which showed that the shipment was conducted by a third party company, which was Iranian. The beneficiary of the LC in the neighbouring State B was acting as front company to the Iranian one, which was the actual beneficial owner from the LC.

- Payment covering goods shipped from a State A in North Africa to a State B neighbouring Iran: a review by the international financial institution of related shipping documents revealed that the goods were in fact in transit to Iran.
- A company A in Iran entered into an agreement with a company B located in a State in the Middle East under which company B agreed to accept or process payments on behalf of company A. Company B had a bank account at a non-Iranian financial institution. Company A informed its customers to direct their payments to company B and informed beneficiaries to expect payments from company B's bank. It is not known how the financial transaction between company B and company A in Iran was conducted.
- An Iranian with an established business in Iran selling goods domestically and abroad, moved out of Iran and continued to own and receive income from his business in Iran. The income was received in the form of wire transactions from small financial institutions located in neighbouring countries. The accounts in these financial institutions from which the wires originated were affiliated with companies located outside Iran (hawala methods may have been used to transfer value between the business in Iran and these companies).

A non-Iranian company A located outside Iran attempted to send a payment to a company B inside Iran: company A sent the payment to a specific account purportedly belonging to company B at a bank inside Iran. The payment was rejected by an international financial institution and a report filed with the authorities. Company A then arranged a second payment for a similar amount, to a beneficiary company C located outside Iran. The beneficiary account number was the same account number as the original company B. It is not known if/how this second attempted payment would have reached company B and no connection between the Iranian company B and the beneficiary company C located outside Iran was revealed by open source searches.

## **Annex 2**

**Dr Jonathan Brewer** is based in New York. He is a Visiting Professor at the Department of War Studies, an Adjunct Senior Fellow at the Center for New American Security, Washington DC, and an Associate Fellow at the Royal United Service's Institute, London. From 2010 to 2015 he worked as financial expert on the UN Panel on Iran created pursuant to resolution 1929 (2010), based in New York. From 1983-2010 he was a member of HM Diplomatic Service. His publications include:

Jonathan Brewer, Proliferation Financing: The Potential Impact of the Nuclear Agreement with Iran on International Controls. Strategic Trade Review, Volume 2, Issue 2, March 2016

Jonathan Brewer, Financial Sanctions on Iran and the Joint Comprehensive Plan of Action, ACAMS Today 9 December 2015

Jonathan Brewer, Sanctions and the Financing of Proliferation: Identifying Circumvention Typologies, ACAMS Today, 9 December 2015

Wyn Q Bowen and Jonathan Brewer, 2011, Iran's Nuclear Challenge, International Affairs, v 87, No 4, 923-943

Jonathan Brewer, 2010, The Private Sector Plays an Important Role in delaying the development of the Iranian Nuclear Programme, Bulletin of the Atomic Scientists, 30 Nov 2010