The Financing of Illicit Arms Transfers and sanctions violations[1]

By Zia Ullah[2]

July 2012

Investigating the financing arrangements behind illicit arms transfers and sanctions violations is critical both to understanding and disrupting this trade. It is axiomatic that there would be no illicit arms trade if there was no form of financing to underpin it. This paper explains how funds are transferred and some of the patterns of sanctions evasion. It also provides practical guidance about 'at risk' financial transactions.

The patterns and networks utilised to traffic small arms and light weapons (SALW) are not dissimilar to those used by state actors to evade sanctions. In fact, the two are intrinsically linked. And there is a direct correlation between the flouting of arms embargoes and the extent to which other sanctions are breached. States such as Iran that go to great lengths to evade economic sanctions are also deeply involved in arms trafficking.

The illicit arms trade is also dependant upon other parties, in particular, intermediaries and brokers operating beneath regulatory scrutiny across multiple jurisdictions. The brokers include notorious international arms merchants such as Viktor Bout, Slobodan Tesic, Rahmat Abdhir and Leonid Minin.[3] Many of the intermediaries, however, are local nationals. One factor that all arms merchants have in common is a profit motivation, for which they need a means to transfer funds. The participants in illicit arms trafficking and sanctions busting use both conventional and non-conventional finance, including informal remittance channels such as hawala banking[4] and the use of goods and commodities as value for exchange, as explained below.

Wire Transfers – How do they work?

Wire transfers are the typical method of effecting cross-border payments between traditional financial institutions. They are used to process payments in cases where the banks of the two parties of a transaction do not have a direct account relationship. Put simply, if I wish to pay $100 from my bank account with HSBC in the UK to my cousin's account in Standard Chartered in Kenya, the payment would be made by way of a wire transfer. If we both bank with HSBC in the same currency, no wire transfer is necessary; the bank simply transfers funds from one account to another by direct deposit. But most

---

[1] This paper is based on the author's presentation at a workshop on 'Implementing Sanctions: Prospects and Problems, held in Nairobi on 23-24 May 2012 and co-directed by the International Institute for Strategic Studies and the Institute for Security Studies.

[2] Zia Ullah is a partner in the Regulatory team and Head of Compliance Advisory at Pannone LLP, a London-based legal firm. He previously worked at Barclays as Group Head of Sanctions and Policy.

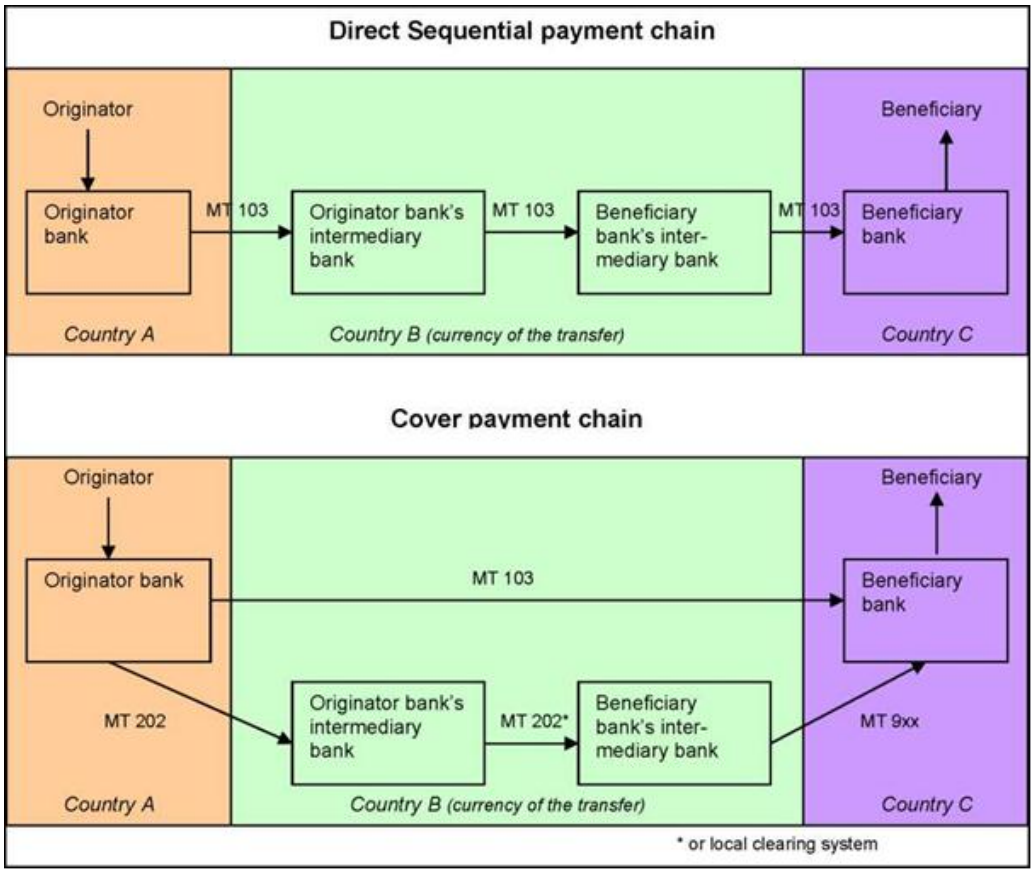
[3] Russian national Viktor Bout, known as the 'merchant of death', was accused of involvement in illegal gems trafficking and of arming factions in several conflicts in Africa and elsewhere. Last year a US court sentenced him to 25 years imprisonment. Serbian national Slobodan Tesic was reportedly involved in brokering significant arms deals between Serbia and Yemen, hiding behind front companies. US national Rahmat Abdhir was convicted of assisting Philippine separatist groups with American military equipment. Ukrainian national Leonid Minin was suspected of brokering arms deals between Russia and Sierra Leone.

[4] For a good explanation of hawala, see Mohammed El-Qorchi, 'The Hawala System', *Finance and Development*, December 2002, Volume 39, Number 4, http://www.gdrc.org/icm/hawala.html.

transactions in the illicit arms trade involve parties that do not have such a direct account relationship.

Wire transfers take two principal forms: the serial payment method and the cover method. Under the serial method, the same information about the transfer is provided in sequence to each of the institutions involved in the process. An MT 103 (Message type 103, used by all institutions that utilise the SWIFT[5] standard) Single Customer Credit Transfer is sent from the ordering customer's financial institution through the correspondent banks to the beneficiary customer's financial institution. The mandatory information fields in the MT 103 are the names of the ordering customer and beneficiary; the value date/currency/ interbank settled amount and the details of charges. Other typical yet optional information fields include the correspondent banks, intermediary institutions, sender and receiver charges, and 'sender to receiver information'.

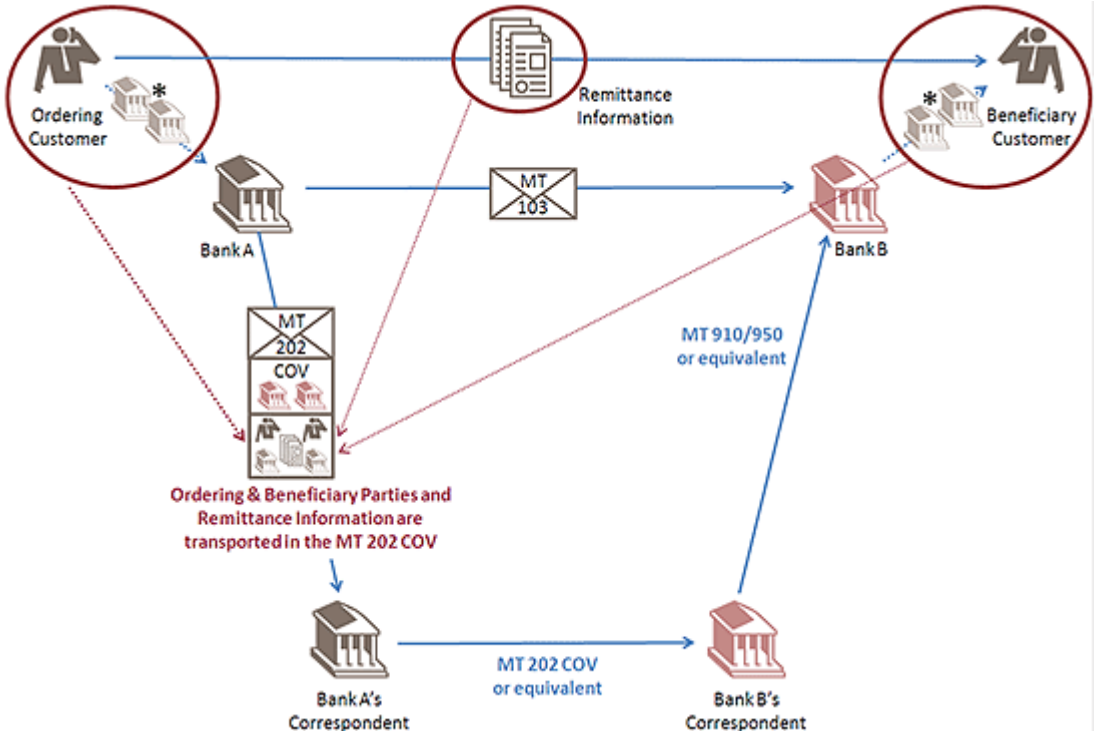
Under the cover method, the MT 103 is exchanged directly between the financial institutions that service the accounts of the two parties, as illustrated in the bottom half of the diagram below. Due to the lack of a direct account relationship in the currency of the transfer, a separate, different kind of covering message, called an MT 202 (now MT202 COV, as discussed below) is sent to clear and settle the payment at the inter-bank level with each of the correspondent and intermediary banks. In our example, HSBC will maintain its own 'correspondent' bank in the US, as will Standard Chartered, which will be used to effect the currency transfer in the US. The payment must transfer through the US, as it is denominated in USD. If the payment had been in Yen, a Japanese correspondent bank would be utilised.



[5]SWIFT (the Society for Worldwide Interbank Financial Telecommunication) supplies secure messaging services and interface software to wholesale financial entities. In March 2012, the EU banned the Iranian Central Bank and about 30 other Iranian financial institutions from using SWIFT.

Source: Basel Committee on Banking Supervision, 'Due diligence and transparency regarding cover payment messages related to cross-border wire transfers, May 2009, http://www.bis.org/publ/bcbs154.pdf.

Obviously, the more information contained in the message, the greater the ability of those looking at it to understand the purpose and nature of the payment. Historically, the MT202 payment method was seen as providing weak controls over international payments as intermediary banks would often not be provided with key information such as originator and beneficiary names and purpose of payment. This made it difficult to screen such messages against lists of entities and individuals who have been designated by international sanctions regimes. From November 2009, the MT202 COV message type has been in use (see below illustration) which has allowed for greater transparency and proper screening to take place of such payments.



Source: SWIFT, 'New standards for cover payments', 19 May 2009, http://www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2009/Newstandardsforcoverpayments.page

The process of filtering and screening is a key function performed by financial institutions. In my example, once I ask my bank to make the payment to my cousin, several types of filtering and screening take place through the chain of banks. These vary from balance screening (to ascertain whether I have enough funds in my account) to more detailed checks, such as sanctions screening. Banks use complex filtering tools to draw out payments that may not comply with regulatory or legal obligations. Such payments are then screened by a variety of manual and non-manual touch-points to ensure that no issues arise. The likelihood that I have been designated by sanctions is minimal since my bank would ordinarily screen my

details (and the details of all its customers) on a frequent basis. However, the details of my cousin will be new to my bank as will my details be new to hers.

It is imperative that effective screening of the payment takes place to ensure that, at a minimum, it is not being made to or from parties that are subject to controls such as economic sanctions. Other reasons for screening include checks as to whether the underlying transaction involves jurisdictions of concern or provides details that require further analysis. If payments were being made by parties ' for the attention of O Bin Laden' one would expect that the banks in question would have sufficient controls to flag the payment for further scrutiny.

If not all optional information is included within the payment message, then the true functionality of screening systems is lessened and the chances of suspect payments falling through the net increase. So in the example above if the sender-to-recipient field is simply left blank, we would not understand that the payment was being made for the attention of O Bin Laden. This was the gap that the new MT202 COV sought to fill, ensuring that intermediary banks see the full transaction picture.

Informal remittance channels

In addition to the formal remittance channel through bank wire transfers, there exist other less formal yet still highly relevant channels that are used by illicit arms traders. Firstly, slightly down the chain from banks are money service businesses (MSB) that have historically been seen as 'simple' *bureaux de change* or remittance operations but which over the past few years have taken on greater prominence in the financial services sector. Their main advantage over the larger banks has tended to lie in the lower costs offered to customers to transfer money across borders. A typical wire transfer through a bank may cost around USD 20-30. MSB typically do not charge any fee, instead making their profit on the difference in currency rates they are able to obtain given the wholesale nature of their businesses. There have been numerous examples of these businesses being used by parties wishing to use less regulated entities to channel funds which are tainted funds, representing the proceeds of criminal activities.

Sitting below the regulated MSB sector are a plethora of dealers operating hawala businesses. These remittance channels have relied upon a trust-based system of making payments between various jurisdictions. Such informal networks often provide a useful, legal means by which displaced peoples can support family members left behind in places where formal banking services are not available. However, hawala are also used by criminals seeking to avoid detection through financial records. One of the perceived benefits of hawala is a lack of formal record-keeping on originator and beneficiary. Theoretically, this enables parties to transact freely without leaving an underlying paper trail.

Increasingly, even these less formal channels are being usurped by innovative methods of financing. Newer systems commonly involve the transfer of value between countries, but outside the legitimate banking system. The 'broker', which may be a financial institution such as a remittance company, or just an ordinary shop selling goods, has an arrangement with a correspondent business in another country. The two businesses have customers that want funds in the other country, and after taking their commission, the two brokers will match the amounts wanted by their respective customers.

The details (which are usually minimal) of the customers who receive the funds are faxed between the brokers (or may simply be the subject of a telephone call), and the customers obtain their funds from the broker at the end of the transaction. The businesses then balance their books, generally by transferring an amount between them over a given time period, for example, once a month (although this could be over a much longer period). Settlement of the net amount owed by one business to the other may not, however, always take place between the two businesses directly; amounts owed between them may be settled by one of the businesses settling an amount owed by the other businesses to a third party, or by the amount being placed or deposited elsewhere for the benefit of the second business. This is known as third party invoicing.

Since the onset of increased economic sanctions against states such as Iran, there has also been an exponential increase in the use of commodity 'bartering' to pay for or finance the supply of goods and services. Commodity exchanges have been in use for millennia, but tended not to be utilised for large purchases such as sales of weaponry. Recently, however, numerous examples have been uncovered highlighting the use of commodities (in particular precious metals and gems) to purchase SALW[6]. The use of such financing provides obvious difficulties to those investigating illicit transfers since the creation of any records relating to the transaction would tend to be confined to the contracting parties and not shared with banks or other institutions.

'Know your customer'

Those arms traffickers that still utilise traditional financing routes often seek to evade detection through the use of front companies to obtain controlled goods, services, or technology. Effective 'customer due diligence' (CDD), otherwise known as 'know your customer' (KYC) information is therefore critical in ensuring that intermediary parties understand exactly with whom and from whom they are conducting business. This is particularly important for regulated financial institutions.

At its most basic level, CDD/KYC relies on identity documentation such as national identity cards, driving licences and passports. More detailed due diligence entails examining corporate information such as incorporation documents, beneficial ownership, shareholdings and other information specific to the particular entity under scrutiny. This information is critical to managing the challenges that arise both from unlicensed arms trafficking and from the use of front companies to conduct such business.

Space is insufficient to cover all the ways in which those involved in illicit trade seek to mask the transactions and the identities of the parties. Let it suffice simply to mention a few recent examples of trafficking cases and the methods attempted to evade detection.

Example 1 – Use of Shell Companies, complex routing and false manifest

In December 2009, Thai authorities, acting on a tip, seized an Ilyushin Il-76 cargo plane cargo plane carrying 35 tonnes of explosives, rocket-propelled grenades, surface-to-air missiles and other weapons on a flight from Pyongyang. The plane was registered to a company in the Republic of Georgia that leased it to a shell

[6] See for example, 'The Charles Taylor Verdict: A Global Witness briefing on a dictator, blood diamonds and timber, and two countries in recovery', Global Witness, 24 May 2012, http://www.globalwitness.org/library/charles-taylor-verdict-global-witness-briefing-dictator-blood-diamonds-and-timber-and-two.

company registered in New Zealand. Multiple flight plans were filed to conceal the final destination of Iran. The cargo manifest listed oil industry spare parts of various types.[7]

Example 2 – Back to Back sales of US-Origin goods

In December 2009 the director of a Singapore firm was found guilty of exporting US parts for Chinook helicopters from the US to Singapore and Malaysia and then re-exporting these items to companies based in Iran, without obtaining the required US licenses. During the arrest, authorities seized catalogues from the China National Precision Machinery Import and Export Corporation (CPMIEC), a company which has been sanctioned by the US because of sale of military hardware to Iran. [8]

Example 3: Iranian shipping lines attempting to circumvent sanctions using foreign-owned vessel [9]

In October 2009, US soldiers in the Gulf of Suez discovered containers of ammunition aboard a German-owned cargo ship chartered by the Iran state-owned shipping corporation Islamic Republic of Iran Shipping Lines. The ship's manifest indicated that the cargo was being transferred from Iran to Syria, in violation of UN Security Council Resolution 1747.

These examples make it clear that there are practical steps that anyone seeking to understand a financing transaction linked to the export or import of goods should undertake. In particular, the questions below provide some starting points in determining whether or not the particular transaction is linked to unlawful conduct such as the trafficking of SALW:

- What is the risk profile of the transaction? (e.g. are the goods dual-use?)
- What countries are involved in each step of the transaction?
- What currencies are being used?
- Who is the ultimate end-user of the goods and where are the goods and the end-user located?
- Is an export licence required?
- Is the documentation accurate?

Red Flags of illicit trade

In carrying out due diligence, financial institutions should be alert to anomalies and inconsistencies that can be a tip-off to an illicit transfer. The following kinds of behaviour can

[7] Daniel Michaels and Margaret Coker, 'Seized arms by Thailand Were Iran-Bound', *Wall Street Journal Asia*, 21 December 2009.

[8] US Department of Justice, Office of Public Affairs, 'Director of Singapore Firm Pleads Guilty to Illegally Exporting Controlled Aircraft Components to Iran', 13 March 2009, http://www.justice.gov/opa/pr/2009/March/09-nsd-227.html.

[9] 'German Ship Transporting Arms for Iran', Spiegel Online, 12 October 2009, http://www.spiegel.de/international/germany/embarrassing-incident-in-gulf-of-suez-german-ship-transporting-arms-for-iran-a-654596.html

serve as 'red flags' that should prompt financial institutions to seek further information or paperwork from those involved in the transaction to ensure that the purpose is legitimate. [10]

Who?

- Wire instructions or payment from or due to parties is not identified on the original documentation;
- The customer or its address is similar to that of an entity or individual designated by the UN or a member state for having been engaged in illicit activity;
- The customer or purchasing agent is reluctant to offer information about the end-use of the goods, services or technology;
- The customer has little or no business background;
- The customer is unfamiliar with a product's performance characteristics;

What/How?

- The importer is willing to pay cash for an expensive item when the terms of sale would normally call for financing;
- The information contained in trade documents and financial flows, such as names, companies, addresses, final destinations etc is internally inconsistent;
- The importer declines the manufacturer's routine support services, such as installation, training and maintenance;
- The importer seeks to use an existing trade finance facility to import very different types of goods, services, or technology than in the past;
- Back-to-back structures are used for selling goods to an emerging market to conceal the end use or end user;
- The customer or counterparty requests amendments to letters of credit that have the effect of removing reference to origin of goods or their ultimate destination;
- The pattern of wire transfer activity shows unusual patterns or has no apparent purpose;
- The importer amends the letter of credit after initial questions to require delivery, for example, to 'any Persian Gulf port' rather than 'Bandar Abbas'.

Where?

- The item ordered is obviously incompatible or inconsistent with the technical level or normal trade pattern of the country to which it is being shipped – for example, semi-conductor manufacturing equipment shipped to a country that has no electronics industry;
- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations;
- A freight forwarding firm is listed as the product's final destination;
- The shipping route is abnormal for the product and destination. For example, a route that ends in a location other than the stated end user's address;
- Documents suggest that a trade transaction may involve a prohibited country even though the customer has not disclosed this possibility, for example, re-export of US-origin aircraft parts to a trade zone in Dubai but guaranteed by a bank in Sudan;
- The transaction involves financial institutions domiciled in countries with weak export control laws or weak enforcement of export control laws;
- Cargo shipped by Iranian owned vessel or otherwise involves a sanctioned country, such as an airport or port in Iran, Syria, or North Korea.

[10] Financial Action Task Force, 'Proliferation Financing Report', 18 June 2008, http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf, p. 54

Remaining challenges

In the end, the ability of concerned states to curb the financing of illegal SALW trafficking is wholly dependant on a number of critical factors. An obvious issue at the heart of illegal arms trafficking is the lack of an agreed international standard. Even if the UN Conference on the Arms Trade Treaty produces a consensus text at the end of July, without the appropriate investment by authorities across the globe into tighter border controls and increased scrutiny of goods moving across these borders, illicit trade will continue.

A second factor is a lack of proper understanding of the techniques being used to disguise this trade. One area that requires much greater co-operation is intelligence about intermediaries. More intense sharing of intelligence across the globe on the key players and their networks is needed in order to effectively investigate and disrupt them.

This is where the interconnectivity with financial crime risk may play a part. Financial institutions already invest huge sums in maintaining vigilance over the traffic passing through their businesses to prevent money laundering, sanctions breaches and corruption. They also have a legal and regulatory obligation to report suspicious activity to the authorities. The information these institutions are able to glean from investigating customer activity, and the activities of other interlocutors, which is passed on to the appropriate authorities, may provide critical intelligence about the SALW trade. If this intelligence can be shared among key stakeholders, the illicit arms trade can be more easily disrupted.