Financial Action Task Force

Groupe d'action financière

PROLIFERATION FINANCING REPORT

18 June 2008

TABLE OF CONTENTS

INTRODUCTION

1. The Proliferation Finance Typology Project develops an understanding of the issues surrounding proliferation financing and provides information that can be used by the FATF to assess the need for policy measures to counter proliferation financing.

2. Pursuant to the FATF's Guidance of 29 June 2007, "Further study of broad-based measures to combat WMD proliferation finance under United Nations Security Council Resolution 1540 (2004) "S/RES/1540 (2004)", the project identifies and analyses the existing threat of proliferation financing; examines existing measures used to counter this threat; and outlines a series of options that could be considered by the FATF to counter proliferation financing, within the framework of existing S/RES/1540 (2004) and S/RES/1673 (2006).

There are financial provisions within paragraphs 2 and 3(d) of S/RES/1540 (2004)'s mandatory Chapter VII obligations that merit further examination by the FATF.

> *2. Decides also that all States, in accordance with their national procedures, shall adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them;*
>
> *3. Decides also that all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall:*
>
> *(d) Establish, develop, review and maintain appropriate effective national export and trans-shipment controls over such items, including appropriate laws and regulations to control export, transit, trans-shipment and re-export and controls on providing funds and services relate to such export and trans-shipment such as financing, and transporting that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations;*

S/RES/1540 (2004) defines a non-state actor as an "*individual or entity, not acting under the lawful authority of any State in conducting activities which come within the scope of this resolution.*"

S/RES/1673 (2006) reiterates the requirements of S/RES/1540 (2004) and emphasizes the importance for all jurisdictions to implement fully that resolution, including provisions regarding the financing of WMD proliferation.

The FATF, while taking into consideration the work of the United Nations 1540 Committee, will conduct further study to:
(a) identify the threat of the financing of WMD proliferation;
(b) analyse the effectiveness of existing measures to counter the threat of the financing of WMD proliferation, and
(c) identify measures (*e.g.* criminalisation measures, broader sanctions, activity-based financial prohibitions or controls or examining the use of financial intelligence) that could be considered in combating WMD proliferation finance within the framework of existing UNSCRs, such as S/RES/1540 (2004).

3. This report has incorporated, *inter alia*, the following into its analysis: 1) jurisdictions' responses to the Proliferation Financing Questionnaire; and 2) the findings of the November 2007 Joint FATF / APG Experts' Meeting on Money Laundering and Terrorist Financing Typologies. The report has also benefited from the discussions that took place at the May (Ottawa) and September (Rome) 2007 WGTM Intersessional Meetings. The Project Team[1] has had opportunities to discuss proliferation financing issues with some representatives of the private sector. Private sector representatives participated at the November 2007 Joint FATF / APG Experts' Proliferation Financing Workshop. The issue of proliferation financing was also discussed at the December 2007 FATF – Private Sector Expert's Meeting on Typologies.

1. ASSESSING THE THREAT OF PROLIFERATION FINANCING

4. The threat of proliferation is significant and the consequences are severe. Proliferation has many guises but ultimately involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programmes, including delivery systems; it poses a significant threat to global security. If appropriate safeguards are not established, maintained and enforced for sensitive materials, technology, services and expertise, they can become accessible to individuals and entities seeking to profit from the acquisition and resale, or for intended use in WMD programmes.

5. They can also find their way into the hands of terrorists willing to employ WMD in acts of terrorism. There is evidence that terrorist organisations continue to pursue chemical, biological, radiological or nuclear (CBRN) capabilities, and it is worrying that their efforts are increasing.[2] In such circumstances, terrorism financing as it relates to providing financial support to terrorist organisations that endeavour to acquire and/or deploy CBRN weapons is then by its nature also contributing to proliferation.

6. Proliferation financing is an element for the movement of proliferation-sensitive items and as such, contributes to global instability and potential catastrophic loss of life if WMD are developed and deployed. Similar to international criminal networks, proliferation support networks are using the international financial system to carry out transactions and business deals.

7. This paper does not seek to define proliferation or proliferation financing. In considering the challenges posed by proliferation financing, this report has looked at issues wider than those set out in S/RES/1540 (2004), strictly defined. The following is a broad working definition of proliferation and proliferation financing for this report only.

> *Proliferation is the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.*
> *This could include, inter alia, technology, goods, software, services or expertise.*
>
> S/RES/1540 (2004) further defines the following:
>
> *Means of delivery: missiles, rockets and other unmanned systems capable of delivering nuclear, chemical, or biological weapons that are specially designed for such use.*
>
> *Related materials: materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for*

[1] The following FATF delegations participated as members of the Project Team: Belgium; Canada; Denmark; France; Germany; Hong Kong, China; Italy; The Netherlands; Switzerland; United Kingdom; United Nations and United States.

[2] *www.cia.gov/library/reports/general-reports-1/CBRN_threat_wo.pdf*
www.csis-scrs.gc.ca/pblctns/prspctvs/200110-eng.asp

the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery.
Proliferation financing is providing financial services for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.

It involves, in particular, the financing of trade in proliferation sensitive goods, but could also include other financial support to individuals or entities engaged in proliferation.

For the purpose of this report, no distinction is made between witting and unwitting actors.

8. The proliferation challenge faced by governments includes the direct technology transfers by governments through nuclear, chemical, biological and missile cooperation or espionage into clandestine efforts to build and acquire WMD capabilities. While there can be legal or other restrictions on information sharing given the sensitive nature of proliferation investigations and intelligence gathering, the report does identify a number of proliferation financing cases. Determining, for example, that a high, medium or low number or value of international financial transactions are facilitating proliferation may be impractical, however, the cases identified in the report show several instances where the international financial system has been used to facilitate proliferation. While it is fact that financial institutions were involved in these transactions it does not per se indicate that they should have been in a position to detect the true nature of the transaction and prevent it.

9. Governments have established numerous multilateral arrangements to detect and prohibit proliferation including the Nuclear Non-Proliferation Treaty[3]; however, as indicated later on in the report, traditional arrangements have not focused on proliferation financing. The detection of even a few proliferation related cases should raise concern, in particular, given the consequences that the use of or threat of using a biological, chemical, radiological or nuclear weapon can have on the international community, including the international financial system.

10. Governments have worked to establish and maintain extensive export controls and safeguards to prevent the acquisition of the required goods, services, technology and expertise by proliferators or their supporters. These controls, including safeguards such as the registration, licensing and pre-approvals for the manufacture and export of a broad range of designated goods, are fundamental in preventing proliferators from acquiring important goods, services, technologies and expertise. However, these controls are not uniform across jurisdictions, and some jurisdictions have yet to implement the requirements mentioned in several international treaties to detect and restrict trade in proliferation sensitive goods and items.

11. In addition, trade globalisation and steady advances in technology are providing fresh challenges for the maintenance of effective export controls. Trade volumes continue to rise and trade patterns are less discernable. Further, there is a growing range of goods and technology that have commercial applications as well as applications for WMD and WMD delivery systems (*i.e.* "dual-use" goods), and while proliferators previously attempted to buy or sell whole manufactured systems with the effective control systems, there is a growing trend to purchase or sell more elementary components. Proliferation networks continuously seek out and exploit weaknesses in the global export control system and international financial system.

12. Export controls are used to *inter alia* prevent dual-use and other sensitive goods (listed and unlisted) from being exported to known individuals and entities that are involved in WMD proliferation-related activities. However, it is challenging for authorities to designate and monitor trade in all relevant "dual-use" goods.

[3] The full range of multilateral arrangements is described in some detail in Annex 4.

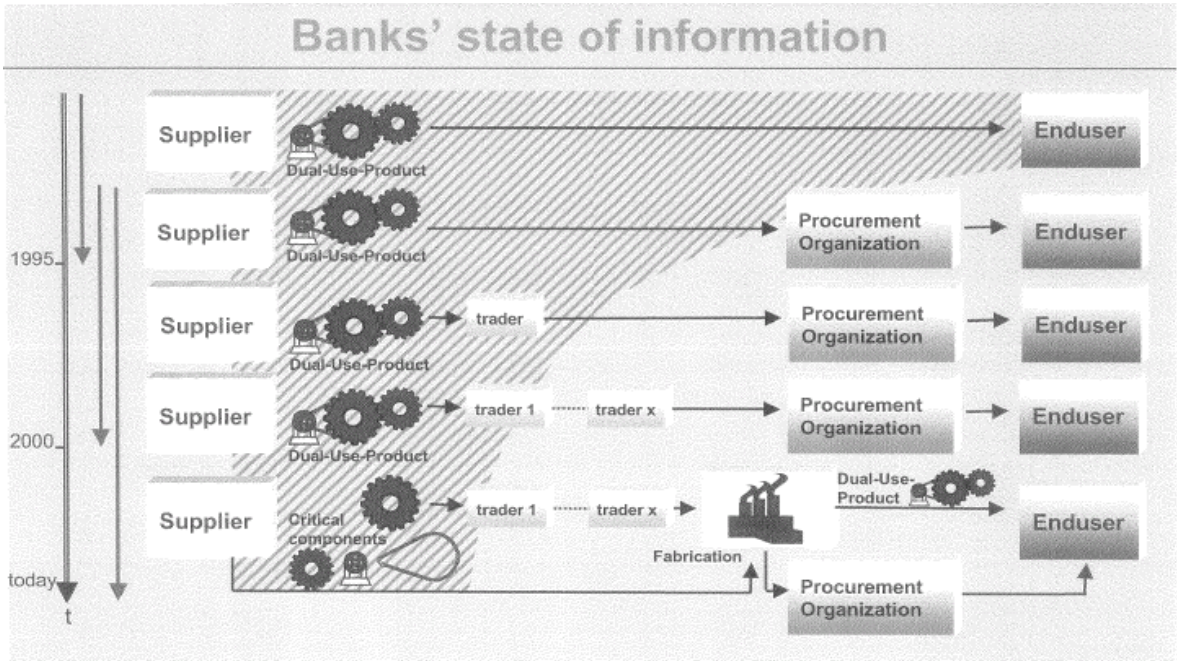
13. Governments are continuously working to further develop these controls while proliferation networks, individuals, entities and countries of concern continue to adapt, using front companies, illicit brokers and illicit means to obtain goods, services, technology and expertise.

14. The multilateral financial prohibitions contained in S/RES/1540 (2004)[4] introduce an additional tool that complement existing counter-proliferation regimes. The diagrams in Annex 2 demonstrate the growing complexity of the procurement process. One or two decades ago financial institutions were in a better position to collect and scrutinise information regarding the ultimate end–use of potentially sensitive proliferation items. However, procurement networks have become more complex over time, increasing: *i)* the number of actors involved; *ii)* the trade in sub-components; and *iii)* the indisputable probability that the true end-users of proliferation sensitive goods will avoid detection. This implies, *inter alia*, the acquisition of technology with the aim of shifting the production capacity to their own country or to generally unwitting production facilities in other countries.

15. With changes to the procurement process and a significant increase in the number of normally innocuous items that now have potential proliferation sensitive applications, it has become far more difficult to assess with a sufficient degree of certainty whether an item will truly be used for civilian purposes. While information that is potentially held by intelligence services has not changed significantly, information held by other entities, including suppliers and financial institutions is greatly diminished. For example, it is common today for suppliers to only have information on intermediary players in the procurement chain. Suppliers deliver dual use products and other critical items that are often not subject to export controls, to traders, brokers and other entities responsible for forwarding on the items as inputs to other facilities where proliferation sensitive goods are then produced.

16. Today, financial institutions have far less information about end-users and ultimate end-uses of items underlying financial transactions. Apart from information that is collected concerning their clients, information in transactions that describe items is generally too vague and/or would require a significant amount of technical knowledge to determine if they were sensitive or not.

17. The following diagram shows the information that is usually available to financial institutions.[5]



Source: Germanv.

[4] And subsequently S/RES/1718(2006), S/RES/1737(2006) and S/RES/1747(2007).

[5] See Annex 2 for further detail.

The scope of proliferation financing

18. Defining the scope of proliferation and proliferation financing for the purposes of this report is both critical and challenging. The report seeks to present the types of proliferation activities that often involve proliferation financing.

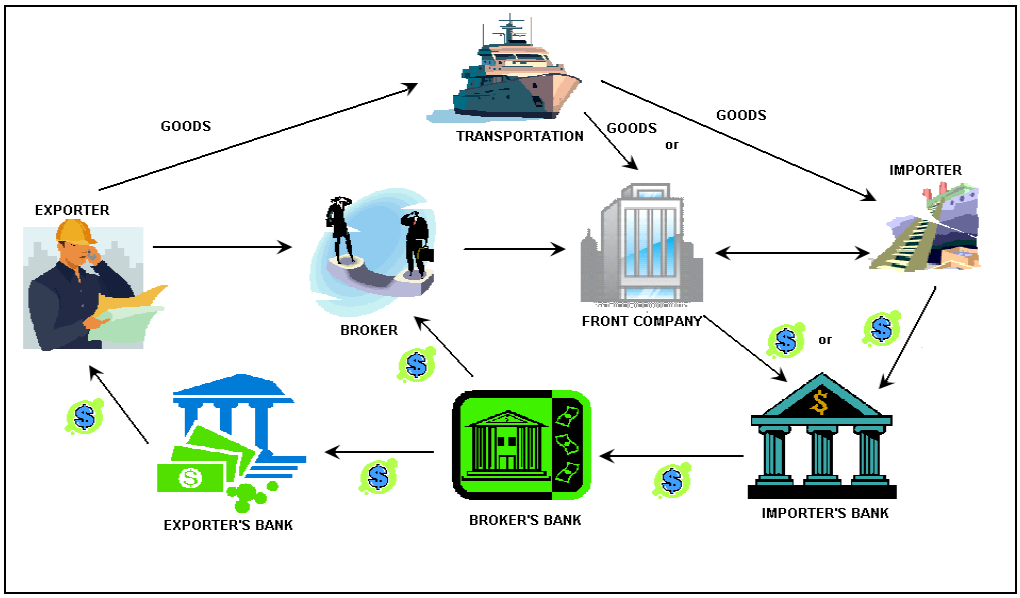
19. Proliferation networks operate globally. Advances in economic integration and in the volume and speed of international travel and trade, facilitate the global transfer of sensitive items by proliferators. Proliferators mask their acquisitions as legitimate trade. They exploit global commerce *e.g.* by operating in countries with high volumes of international trade or utilising free-trade zones, where their illicit procurements and shipments are more likely to escape scrutiny. However, in reaction to this phenomenon, jurisdictions with a highly developed and efficient export control system make enhanced efforts to control these transactions.

20. The following diagram illustrates a basic foreign trade pattern which is routinely used in export financing. Proliferators may abuse this typical trade pattern to disguise their real intentions. It is a starting point for subsequent illustrations and cases that provide a more dynamic snapshot of individuals, entities, products, and documents proliferators may use and exploit, as well as the financing mechanisms they use to facilitate their trade.

OVERVIEW OF A FOREIGN TRADE PATTERN ABUSED FOR PROLIFERATION

An importer may arrange for the shipment of goods directly with an exporter or could use a front company, broker or both a front company and a broker.

Similarly, payments may be settled with a manufacturer's bank either: directly; using a Front Company; using a Broker; or the manufacturer may arrange for payment using Letter of Credit or other payment method.



Source: Canada.

21. Proliferators rely on support structures[6] that exploit a number of channels to facilitate the purchase, sale, export or import of sensitive goods. As with most illicit trafficking, proliferation networks work to conceal the end-user of traded goods, the goods themselves as well as the entities involved and associated financial transactions.

6 More information provided in the section "Witting and Unwitting Actors".

22. To ensure that authorities do not detect the real end-use of sensitive goods being exported, networks may use intermediaries and front companies to arrange for the trade and export of goods by witting or unwitting companies. However, the use of intermediaries is not in itself an indication for proliferation financing. Exporters employ intermediaries for legitimate purposes. When exporting out of or through jurisdictions with well-developed export control regimes, intermediaries and front companies may use fraudulent documents, such as false end-use certificates, forged export and re-export certificates. Couriers or other facilitators may be used to ensure that the transfer of goods, in particular at main transit points, avoids inspection to ensure safe entry of the goods by land, sea, or air.

Activities relevant to this report

23. Weapons of mass destruction proliferation, including the transfer of complete systems or the transfer of components; dual-use goods, services, technology, expertise and training, that could be used to develop weapons or delivery capability is the primary focus of this report. The theft of high value materials from authorised storage facilities with the intention of resale should also be considered a proliferation-relevant activity.

Dual-use goods

24. Proliferators purchase dual-use items, many of which are controlled under international export control regimes. In contrast to trafficking in nuclear or radiological material, these purchases are mostly settled using a range of financial transactions, normally through the formal financial sector.

25. Dual-use goods are items that have both commercial and military or proliferation applications. This can include goods that are components of a weapon, or those that would be used in the manufacture of a weapon (*e.g.* certain machine tools that are used for repairing automobiles can also be used to manufacture certain component parts of missiles).

26. Export control systems are continuously updated and expanded to incorporate new goods and technologies. This has forced proliferators in some cases to adopt a different strategy to select, where feasible, elementary components rather than complete subassemblies[7] to elude authorities. However, a high level of technical expertise is often required to integrate various elementary goods into a full assembly, and as such, proliferation networks may continue to attempt to illegally purchase subassemblies or complete systems. They may even attempt to acquire the manufacturing company.

27. Dual-use goods destined for proliferation use are difficult to identify even when detailed information on a particular good is available. Regardless of the amount of information provided for a particular good, highly specialised knowledge and experience is often needed to determine if a good may be used for proliferation. The table below includes a small subset of the kinds of items – with only minimal information – that are often classified as dual-use by jurisdictions, it is by no means an exhaustive list of dual-use items, as national dual-use goods lists often contain hundreds of items, as well as the technology used to design, manufacture or use such items. Dual-use items can be described in common terms with many uses – such as "scrubbers" – or in very specific terms with more specific proliferation uses – such as metals with certain characteristics. Further, many of the goods listed in this table are only regarded as dual-use if they measure-up to very precise performance specifications.

[7] A subassembly is defined as a major subdivision of an assembly consisting of a package of parts, elements, and circuits that perform a specific function.

Table 1. Select examples of general dual-use items

Nuclear	*Chemical*	*Biological*	*Missile and delivery*
Centrifuges	Scrubbers	Bacterial strains	Accelerometers
High-speed cameras	Mixing vessels	Fermenters	Aluminium alloys
Composites	Centrifuges	Filters	Aluminium powders
Maraging steel	Elevators	Mills	Gyroscopes
Mass spectrometers	Condensers	Presses	Isostatic presses
Pulse generators	Connectors	Pumps	Composites
X-ray flash apparatus	Coolers	Spray dryers	Maraging steel
Pressure gauges	Precursors	Tanks	Homing devices
Ignition	Pumps	Growth media	Oxidants
Vacuum pumps	Reactors		Machine tools
	Heat exchanges		

Source: "Proliferation of weapons of mass destruction", Report from the Swedish Security Service.

Transhipment and diversion

28. Transhipment centres, commonly known as 'hubs' are cargo-sorting and redistribution destinations through which much international trade is routed. Examples of major international hubs include the Netherlands (Rotterdam), the UK (Felixstowe), Hong Kong, Singapore, and Malaysia (Port Klang). Free trade zones are destinations where goods pass through on route to their final destination. Free trade zones, while not always transhipment hubs, are sometimes used by exporters as the landing post for goods destined for end-users in nearby jurisdictions. Examples include the United Arab Emirates (Jebel Ali free port), Malta and Cyprus.

29. Routing goods through transhipment hubs offers a number of advantages to those seeking to facilitate international trade. It is common practice amongst cargo shippers and helps lower shipping costs by reducing the number of ship movements required. Although transhipment routes are often highly complex, with goods travelling through many hubs, they provide the opportunity to link up with other vessels going directly to the end-user destination and do not require specially charted ships to be commissioned or to travel empty – cutting the cost to the importer. Goods travelling through a hub may be small volume – single packages or containers. Many hubs, like free trade zones, have the additional advantage of being close to their eventual cargo destination.

30. For the procurer of illicit goods seeking to avoid detection, the advantages of Free Trade Zones and Transhipment Hubs are that less stringent export controls are often applied by states to goods being transhipped or routed through free trade zones than to goods entering their territory through other means. As goods do not officially enter the economy in question they may be beyond effective customs and police control. The final journey may be by smaller cargo vessel or it may be completed by land or air. Although certain destinations maintain accurate data for cargo passing through their ports for commercial reasons the constant rerouting of goods can make effective tracking of cargo difficult.

31. Diversion occurs when the supplier, broker or end-user deliberately tries to conceal the eventual destination of a particular shipment. For instance, when diverted goods pass through a third country, an individual in that country who is aware of the true destination of the goods seeks to establish himself as a false end-user. Entities or persons seeking to conceal the true end-user have the best chance of doing so by diverting or routing goods through third countries with weak (or non-existent) controls. Diversion points used by proliferators will often be ports where national shipping carriers call and where goods can be passed on to other cargo shippers on route to their final destination.

32. While transhipment and diversion make traditional counter-proliferation controls harder to enforce it can result in a financial intelligence trail for investigators and customs authorities to follow breaches of export control law. Financial flows required to move goods from one place to the next could provide authorities with supplementary information to link up entities of concern with transport routes and ultimate end-users.

Proliferators' use of the formal financial sector

33. Some elements of proliferation support networks may operate for financial gain and the formal financial sector can be abused by networks to carry out transactions and business dealings worldwide. Apart from transaction and business activities in the informal financial sector, proliferation financing can involve traditional trade finance products and transactions.

34. There have been incidences where proliferation-related transactions are settled through opaque cash or "barter-like" settlements involving goods such as oil, sensitive military goods or other proliferation sensitive goods. Cash may be used by proliferators to avoid detection by financial monitoring systems. Further, the cash used in payments may have been obtained through illegal activity. Cash payments for goods do not create financial (paper or electronic) trails and therefore do not contribute financial information that may be useful in identifying and combating proliferation activity.

35. However, it is important for proliferators to have access to the international financial system under most circumstances. Purchases must appear to be legitimate if proliferators are to elude suspicions and they often exploit commercial companies with legitimate businesses.

36. While there are cases where proliferators have exchanged suitcases of cash, this is not cost effective or efficient and is certainly suspicious. Companies being used unwittingly are aware of the sensitivities surrounding their products and are often required to exercise due diligence with purchasing parties. It would be quite suspicious, for example, if an individual tried to purchase a piece of machining equipment with cash.

37. International trade has well established instruments to facilitate imports and exports while mitigating business risks, including the general level of trust between parties engaged in a transaction. Trust is exploited by proliferators to ensure the minimum amount of scrutiny. Traditional trade financing contracts clearly define the specific terms of trade and ensure each party that the other will follow through on their end of the arrangement. The most common payment methods include open account payment, pre-payment, documents against payment and letters of credit. Trade can also be financed through more direct means via credit. These are discussed in more detail below.

38. Proliferation networks also use financial flows to pay intermediaries and suppliers outside the network. Similar to actors that supply proliferation networks, financial institutions are usually unwitting facilitators of proliferation, as a consequence of the complexity of dual-use goods, the involvement of illicit intermediaries, front companies and illegal trade brokers.

Survey results on disrupting and deterring proliferation and proliferation financing[8]

39. Some jurisdictions raised the following general risk factors which might make a jurisdiction vulnerable to proliferation financing, in response to the Proliferation Financing Questionnaire (the survey). The most significant risk factors include: laws or enforcement capacity, its size, openness, industrial make-up and volume of trade with respect to the economy and/or geography. Specific factors raised in the survey responses include:

[8] A survey was sent to all jurisdictions on 1 October 2007 and this report reflects the responses of 20 jurisdictions.

- Weak AML/CFT controls and/or weak regulation of the financial sector.
- Weak or non-existent export control regime and/or weak enforcement of existing export control regime.
- Non-party to relevant international conventions and treaties regarding the non-proliferation of weapons of mass destruction.
- Lack of implementation of relevant UNSCRs.
- The presence of industry that produces WMD components or dual-use goods.
- A relatively well-developed financial system or an open economy.
- The nature of the jurisdiction's export trade (volumes and geographical end-users).
- A financial sector that provides a high number of financial services in support of international trade.
- Geographic proximity, significant trade facilitation capacity (*e.g.* trade hub or free trade zone), or other factors causing a jurisdiction to be used frequently as a transshipment point from countries that manufacture dual-use goods to countries of proliferation concern.
- Movement of people and funds to or from high-risk countries can provide a convenient cover for activities related to proliferation financing.
- Lack of working coordination between the customs authority and the export licensing authority of a specific jurisdiction.
- A jurisdiction that has secondary markets for technology.

40. Most jurisdictions responded that any financial services related to international trade, including through products such as letters of credit, could be abused to finance trade in proliferation-sensitive goods. Financial institutions providing trade finance services are at risk of being abused for proliferation financing with financial services and products such as letters of credit (or documentary credits), loans and electronic funds transfers. It was noted that *hawala* and money remittance services and the insurance sector were at risk for proliferation financing and identified that proliferation networks may use cash couriers to finance proliferation.

41. A number of jurisdictions indicated that general risks, such as having a highly developed industry and financial sector, will increase vulnerabilities should no efficient export control system exist. When asked to assess the effectiveness of export controls in their own jurisdiction, respondents generally considered their system to be adequate.

2. WITTING AND UNWITTING ACTORS

42. Proliferators abuse typical trade structures to facilitate their activities, which include supporters, financiers, logistical support, front companies, assets, shippers and facilitators. Entities that are knowingly engaged in proliferation, such as a front company, may also be involved in legitimate business. Other actors used by a network may knowingly support proliferation, be "wilfully blind" that they are being used for illicit purposes, or are truly unwitting actors. When an entity is engaged in both legitimate and illicit trade it may be less likely for financial institutions to suspect illegal activity.

Front and Other Companies

43. In individual cases, proliferation networks have employed companies to conceal the true end-use or end-user of traded goods. Most front companies are sensitive to public exposure and disruption of legitimate activities.

44. Front companies established by proliferators conduct transactions similar to those of companies engaged in legitimate business. Front companies used by proliferators may be similar to those established by money launderers. As is the practice of other criminal organisations, proliferators create companies for a seemingly legitimate commercial purpose and commingle illegal funds with funds generated by legal commercial activity. In some cases, front companies established by proliferators do not engage in any legal activity at all. Front companies may use fraudulent accounting practices and establish various offshore entities in jurisdictions with lax controls to disguise illegal operations.[9] Proliferators are also known to change the names of front companies, or to use multiple names for the same front company, to prevent the detection of the companies' association with proliferation – or other illicit activity.

45. Front companies used by proliferators are often located in a major trading hub of a foreign jurisdiction with lax export controls but may also be found in jurisdictions with more established controls. They can be shell corporations with a fictitious business and physical location or can have normal commercial and industrial operations.

46. Front companies can arrange shipping services, routing or re-routing goods acquired by the importer or its intermediary. The same and/or additional companies can also be located in jurisdictions with weak financial controls, enabling related financial transactions to settle the underlying trade without detection.

47. In exceptional cases, front companies may seek complicity within a particular jurisdiction's government for signoff by national authorities, by production of false cargo manifests to misdirect customs, law enforcement, and intelligence as to the true nature of the goods being exported and their end-use.

Brokers

48. Brokers are involved in the negotiation or arrangement of transactions that may involve the transfer of items (often between 3rd countries) or who buy, sell or arrange the transfer of such items that are in their ownership. In addition they may also become involved in ancillary activities that facilitate the movement of items such as, but not limited to: *i)* providing insurance; *ii)* marketing; *iii)* financing; and *iv)* transportation / logistics. Illicit brokers illegally participate in proliferation by circumventing existing controls and obfuscating trade activities.

49. Brokers used by proliferation networks are often individuals relying on simple commercial structures, who are very mobile (financially and geographically) so that they can operate from any jurisdiction.

Other Intermediaries

50. Intermediaries may include companies and individuals that purchase or sell sensitive goods for further manufacture or redistribution. Intermediaries may have a particular knowledge of a jurisdiction's commercial infrastructure. Intermediaries that are knowingly engaged in proliferation will use this knowledge to exploit vulnerabilities in export control systems to the advantage of the proliferator.

Financial Institutions

51. Proliferation networks may use financial institutions to hold and transfer funds, settle trade and pay for services. Proliferation networks may use both private and public financial institutions for international transactions. States seeking to acquire WMDs may also use foreign branches and subsidiaries of state-owned banks for proliferation finance-related activities, giving these institutions

[9] FATF (2003), FATF (2006).

the responsibility of managing funds and making and receiving payments associated with proliferation-related procurement or other transactions. These subsidiaries may be engaged in both legitimate and illegitimate transactions.

Financial institution settlement of international trade transactions[10]

52. Financial institutions support international trade in three main ways:

- A financial institution's products and services are used to settle international trade transactions. These products and services range from payment transfers[11] from the importer to the exporter to more sophisticated financial products, such as a letters of credit[12], documentary collections and guarantees.
- The financial sector provides export finance to bridge the time between the need of funds for production, transportation etc. and the payment for such products by the importer. Banks and other export credit agencies provide loans and credit to traders to enable them to purchase and resale goods or equipment.
- The financial sector may provide insurance against certain risks involved in the trading process. Insurance instruments can protect exporters against the non-payment of buyers and insure against non-compliance by the seller and risks arising from government policy changes (*i.e.* political risk).

53. The role of financial institutions in trade finance is not limited to the provision of financial products. In addition, financial institutions provide valuable information to investors and traders depending on the financial service they provide to their client. They may inform their clients about present and future money and capital market conditions. And they operate through established international banking relationships with correspondents, which give their clients greater assurance about the legitimacy of their trading partners. While correspondent banks are used to facilitate trade transactions, the use of these banks does not provide legitimacy to the commercial parties to a transaction. Depending on the trade finance process used, it may provide a greater assurance of payment, however, it does not account for the legitimacy of a trading partner. This role feeds directly into the provision of the three groups of products and it will not be discussed separately.

Trade Settlement

54. In all business transactions, there is some commercial risk. However, in the international context, this risk can be magnified, as information about foreign companies (*e.g.* importers, foreign banks, economic conditions and foreign laws) would likely be less familiar to the exporter and his bank, than in respect of domestic clients. This applies equally to both exporters and importers.

55. For the exporter, commercial risks include the importer not accepting the merchandise or not paying for it once it is accepted. The importer risks that the exporter does not deliver the products at the agreed quality and time. In both cases, the capital invested in the purchase or sale – be it out of companies' own funds or through a credit facility – is at risk.

56. A key consideration in mitigating commercial risk is the choice of trade financing instrument. Traders typically choose from three main methods for settling trade transactions, depending on the extent of commercial risk: *i)* Clean Payments (open account and payment in advance), *ii)* Documentary Collections, and *iii)* Letters of Credit.

---

10 This section significantly relies on information by Hinkelman, E. G., (2002b)

11 This would include wire payments.

12 The term letter of credit is a broad term that includes both Commercial Letters of Credit (typically used for the purchase and sale of goods and services) and Standby Letters of Credit (used for various purposes to guarantee a payment and commonly used to guarantee the purchase and sale of goods and services).

57. It is estimated that about 80% of global trade is conducted not using the traditional process of letters of credit and collections and may be simply clean payments processed through financial institutions. Of the remaining 20% of global trade it is estimated that as much as ten percent may be transacted completely outside the traditional financial system.[13]

58. The following is a description of the three main methods of settling trade transactions.

(i) Clean Payments

59. Clean Payments are typically limited to transactions between well-established, ongoing trading partners or other partnerships where significant trust exists between the importer and exporter. In clean payment transactions, the role of the financial institutions is limited to the transfer of funds. Documents, such as title documents and invoices, are transferred between trading parties without a financial institution acting as the intermediary. Clean payments may be used for any purpose and are not specific to transactions between an importer and exporter.

60. As mentioned, the use of open account transactions by entities engaged in international trade is most commonly used. The decline in use of letters of credit or other trade finance vehicles is in relation to the overall growth in world trade. The actual transaction volume for letters of credit has remained relatively stable over time while the volume of world trade has grown.

61. A significant advantage of clean payments is that the administrative costs, including the time required to settle the transaction and the fee paid to a financial institution, are minimal.

62. The two most common types of clean payments are open account and payment in advance.

(i)(a) Open Account

63. An open account transaction involves the exporter shipping the goods and sending the trade documents directly to the importer. Once the goods are received, the importer arranges through its financial institution to forward payment to the exporter. In this arrangement, the exporter bears all risk and, in the absence of other financial arrangements, cannot access the funds until payment is received from the importer.

(i)(b) Payment in Advance (full or partial)

64. A payment in advance transaction reverses the order of an open account transaction. The first step involves the importer providing payment to the exporter as agreed. Once the exporter receives payment, the goods are shipped and the documents sent to the importer. In this arrangement, the importer bears all risk. In addition, there is an opportunity cost to the importer of using the funds prior to the goods being received.

65. Financial institutions participating in open account transactions will monitor transactions in accordance with domestic anti-money laundering and counter-terrorist financing regulations. This typically involves undertaking the appropriate customer due diligence (CDD) and record keeping as outlined in FATF recommendations and local regulatory requirements.

66. The level of scrutiny and information available on the underlying transaction will depend on the financial institution's exposure to credit and reputation risk associated with the nature of the customer relationship or its participation in the transaction. For example, because an institution's risk exposure when participating in an open account transaction is low, it would not likely scrutinise (or even see) the documents supporting the transaction (*e.g.* bills of lading or invoices).

[13] International Chamber of Commerce

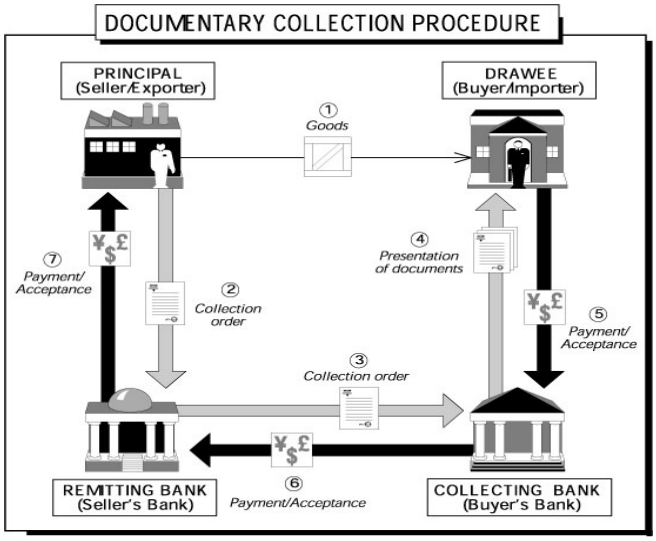
(ii) Documentary Collections

67. Documentary Collections involve the exporter transferring documents (such as an invoice and transportation documents) through exporter's bank to the bank designated by the importer. The importer is able to retrieve the documents once it has made payment or accepted drafts for future payment and obtain release of the goods. In simple terms, banks act as intermediaries to collect payment from the buyer in exchange for the transfer of documents that enable the holder to take possession of the goods. In a typical collections transaction, the bank does not have title or control over the goods.

68. As in the case of an open account transaction, there is a risk of non-payment by the importer, because financial institutions involved in the transaction do not guarantee payment or assume credit risk. The role of financial institutions is to act as an intermediary to forward documents from the exporter to the importer upon receipt of payment (Documents against Payment) or the importer's promise of payment at a later date (Documents against Acceptance). The banks are under no obligation to authenticate documents.

Documentary Collection Process

69. The documentary collection procedure involves the step-by-step exchange of documents giving title to goods for either cash or a contracted promise to pay at a later time. The diagram following the description below illustrates by way of example only each numbered step.



Contract for the purchase and sale of goods – The Buyer and Seller agree on the terms of sale of goods: (a) specifying a documentary collection as the means of payment, (b) naming a Collecting Bank (usually the buyer's bank), and (c) listing required documents.

(1) Seller ships the goods – The Seller ships the goods to the Buyer and obtains a transport document from the shipping firm/agent. Various types of transport documents (which may or may not be negotiable) are used in international trade and only where required by the underlying transaction is a negotiable document used.

(2) Seller presents documents to Remitting Bank – The Seller prepares and presents a document package to his bank (the Remitting Bank) consisting of: (a) a collection order specifying the terms and conditions under which the bank is to hand over documents to the Buyer and receive payment, and (b) other documents (*e.g.* transport document, insurance document, certificate of origin, inspection certificate, etc.) as required by the buyer.

(3) Remitting Bank sends documents to Collecting Bank – The Remitting Bank sends the documentation package by mail or by courier to the Collecting Bank in the Buyer's country[14] with instructions to present them to the Buyer and collect payment.

(4) The Collecting Bank reviews and provides documents to Buyer – The Collecting Bank (a) reviews the documents making sure they appear to be as described in the collection order, (b) notifies the Buyer about the terms and conditions of the collection order, and (c) releases the documents once the

[14] While a collecting bank may be in the buyer's country it need not be.

payment or acceptance conditions have been met. Acceptances under documentary collections are known as "Trade Acceptances" which, when accepted (by the Buyer), only carry the obligation of the buyer as opposed to a "Bankers Acceptance' commonly used under a letter of credit which carries the obligation of a bank.

(5) Buyer provides payment to Collecting Bank – The Buyer (a) makes a cash payment, or if the collection order allows, signs an acceptance (promise of the Buyer to pay at a future date) and (b) receives the documents and takes possession of the shipment.

(6) Collecting Bank provides payment to Remitting Bank – The Collecting Bank pays the Remitting Bank either with an immediate payment or, at the maturity date of the accepted bill of exchange if it receives payment from the Buyer.

(7) The Remitting Bank pays the Seller.

70. See Annex 7 for a description of the document that accompany a Documentary Collection transaction.

(iii) Letters of Credit

71. A letter of credit (also known widely as a documentary credit) is the written and almost always irrevocable[15] promise of a bank to pay a seller the amount specified in the credit, subject to compliance with the stated terms. The fact the seller is relying on the promise of a bank rather than the buyer for payment is the biggest distinction between a letter of credit and a documentary collection transaction.

72. Documentary credits provide a high level of protection and security to both buyers and sellers engaged in international trade. The seller is assured that payment will be made by a bank so long as the terms and conditions of the credit are met. The buyer is assured that payment will be released to the seller only after the bank has received the documents called for in the credit and those documents comply with the terms and conditions of the credit.

73. Although documentary credits provide good protection and are the preferred means of payment in many international transactions, they do have limitations. They do not, for example, ensure that the goods actually shipped are as ordered. It is up to the parties to settle questions of this nature between themselves. Documentary credits will also have higher transaction costs than other settlement methods. A letter of credit is an international established practice offering the best level of legal / contractual certainty, and therefore constitutes one of the most reliable payment methods for international transactions. A core element of the letter of credit is the concept that banks deal with documents and not with goods, services or performance to which the documents may relate[16] and banks examine documents presented under letters of credit "on their face"[17] in compliance with international standards banking practice.[18]

74. While this covers the traditional commercial letter of credit, standby letters of credit and bank guarantees are often frequently used for the purchase of goods and services internationally.

---

15 Revocable credits are rarely used today and are no longer included in international rules such as the International Chamber of Commerce Unified Customs and Practise (UCP).

16 UCP 600 Article 5.

17 UCP for Documentary Credit, Article 14(a).

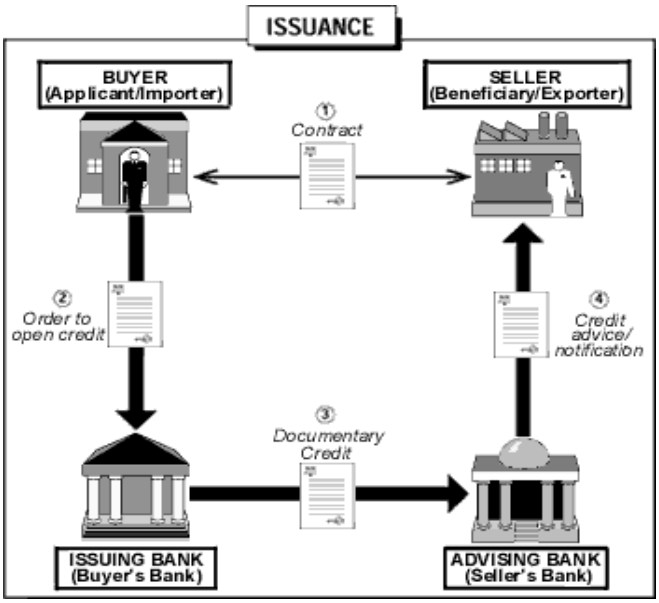
18 UCP Article 14 (d).

Basic Documentary Credit Procedure

75. The documentary credit procedure involves the step-by-step exchange of documents required by the credit[19] for either cash or a contracted promise to pay at a later time. There are four basic groupings of steps in the procedure: (a) Issuance; (b) Amendment, if any; (c) Utilisation; and (d) Settlement. A simplified example follows:

(a) Issuance

76. Issuance describes the process of the buyer's applying for and the issuing bank opening a documentary credit and the issuing bank's formal notification of the seller either directly or through an advising bank.



(1) Contract – The Buyer and Seller agree on the terms of sale: (a) specifying a documentary credit as the means of payment, (b) naming an advising bank (usually the Seller's bank), and (c) listing required documents. The naming of an Advising Bank may be done by the buyer or may be chosen by the issuing bank based on its correspondent network

(2) Issue Credit – The Buyer applies to his bank (Issuing Bank) and the issuing bank opens a documentary credit naming the Seller as beneficiary based on specific terms and conditions that are listed in the credit.

(3) Documentary Credit – The Issuing Bank sends the documentary credit either directly or through an advising bank named in the credit. An advising bank may act as a bank nominated to pay or negotiate (nominated bank) under the credit or act as a confirming bank where it adds its undertaking to the credit in addition to that of the issuing bank. Only in those cases where an advising bank is not nominated to negotiate or confirm the credit is the role of that bank simply an advising bank.

(4) Credit Advice - The advising, nominating or confirming bank informs (advises) the seller of the documentary credit.

(b) Amendment

77. Amendment describes the process whereby the terms and conditions of a documentary credit may be modified after the credit has been issued.

78. When the seller receives the documentary credit, it may disagree with the terms and conditions (*e.g.* the transaction price listed in the credit may be lower than the originally agreed upon price) or may be unable to meet specific requirements of the credit (*e.g.* the time may be too short to effect shipment).

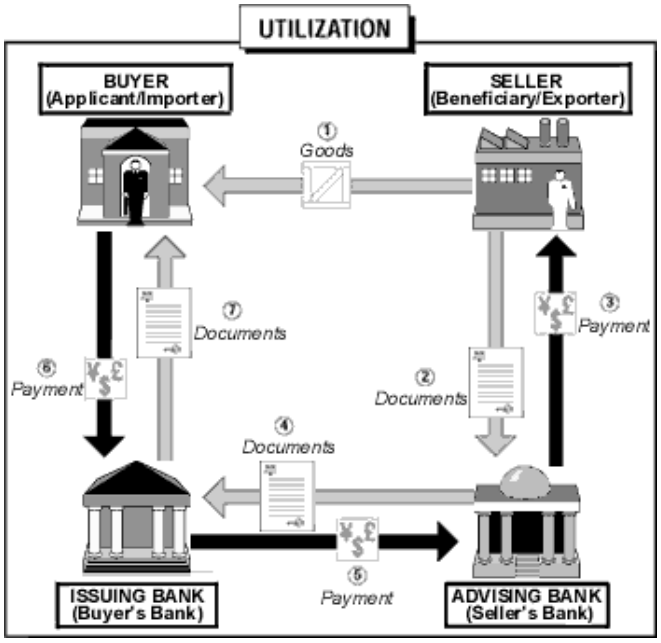
79. If the seller wants to amend the terms prior to transacting, the seller can request these from the buyer. It is at the discretion of the buyer to adopt the proposed amendments and request an amendment to be issued by the issuing bank. An amended letter of credit would be issued by the issuing bank to the seller through the same channel as the original documentary letter of credit.

[19] Title only transfers if a document of title is required under the credit.

Amendments to a letter of credit require the agreement of the issuing bank, confirming bank (if any), and the beneficiary to become effective.

(c) Utilisation

80. Utilisation describes the procedure for the seller's shipping of the goods, the transfer of documents from the seller to the buyer through the banks (presentation), and the transfer of the payment from the buyer to the seller through the banks (settlement). For example:



(1) Seller ships goods – The seller (beneficiary) ships the goods to the buyer and obtains the documents required by the letter of credit.

(2) Seller presents documents to Advising or Confirming Bank or directly to the Issuing Bank – The seller prepares and presents a document package to his bank (the advising or confirming bank) consisting of (a) the transport document if required by the credit, and (b) other documents (*e.g.* commercial invoice, insurance document, certificate of origin, inspection certificate, etc.) as required by the documentary credit.

(3) Nominated or Confirming Bank reviews documents and pays Seller - The nominating or confirming bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit and (b) pays the seller (based upon the terms of the credit) which may mean that payment does not occur until after (5). An advising bank does not normally examine the documents, but simply forwards them on to the confirming or issuing bank for their examination.

(4) Advising, Nominated or Confirming Bank transfers documents to Issuing Bank – The Advising, Nominated or Confirming bank sends the documentation by mail or by courier to the issuing bank.

(5) Issuing Bank reviews documents and reimburses the Nominated or Confirming Bank or makes payment to the beneficiary through the Advising Bank – The Issuing Bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit, under advice to the Buyer that the documents have arrived, and (b) pays the beneficiary through the advising bank or reimburses the nominated or confirming bank (based upon the terms of the credit) and,

(6) Buyer reimburses the Issuing Bank – The Buyer immediately reimburses the amount paid by the issuing bank or is granted a credit by the issuing bank allowing it to reimburse the issuing bank at a later date.

(7) Buyer receives documents and access to goods – The Issuing Bank sends the documents by mail or courier to the buyer who then takes possession of the shipment.

(d) Settlement

81. Settlement describes the different ways in which payment may be effected to the seller from the buyer through the banks. The form of payment is specified in the original credit, and must therefore be accepted by the seller. The following are common settlement methods:

- The Sight Credit (Settlement by Payment) – In a sight credit, the value of the credit is available to the exporter as soon as the terms and conditions of the credit have been met (as soon as the prescribed document package has been presented to and checked by the issuing, nominated or confirming bank and found to be conforming to the terms and conditions of the credit) or once the advising bank has received the funds from the issuing bank (unconfirmed). Payment may be affected directly by the nominated bank or confirming bank upon their examination of the documents and they are reimbursed for that payment by the issuing bank.
- The Usance Credit (Settlement by Acceptance) – In a Usance Credit, the beneficiary presents the required document package to the bank along with a time draft drawn on the issuing, nominated or confirming bank, or a third bank for the value of the credit. Once the documents have been found to be in order, the draft is accepted by the bank upon which it is drawn (the draft is now called an acceptance) and it may be returned to the seller who holds it until maturity.
- The Deferred Payment Credit - In a deferred payment credit the issuing bank and/or the nominated or confirming bank accepts the documents and pays the beneficiary after a set period of time. The issuing, nominated or confirming bank makes the payment at the specified time, when the terms and conditions of the credit have been met.
- Negotiation is the term used where a bank other than the issuing bank agrees to advance funds or discount drafts to the exporter before the issuing bank has paid. Discounting an accepted draft has the same effect.

82. A letter of credit will normally require the presentation of several documents including a Draft[20], Commercial Invoice, Transport Document, Insurance Document, Certificates of Origin and Inspection, Packing and Weight Lists. Annex 7 provides some detail on the kinds of information that may be contained in each of these documents.

Export Financing

83. Through a variety of sources and structures, exporters can obtain financing (working capital) to facilitate their trading activities and bridge the time from which they spend money on an export activity (for example, securing an export order) until the moment of payment. Working capital financing can be applied to the manufacture and development of goods prior to shipment, or be applied to business activities following shipment but prior to receipt of payment.

84. The following section briefly describes the following types of trade finance:

(a) Direct Loans or general credit facility.
(b) Note Purchases (also known as forfaiting).
(c) Factoring.
(d) Guarantees.

(a) Direct Loans

85. Acting independently or as part of a syndicate, financial institutions and other entities offer loans to facilitate export transactions. There are two basic types of loans. Buyer credit involves an arrangement to finance exports generally related to a specific contract. Supplier credit transactions are structured to provide the exporter with the ability to provide its buyer with extended payment terms. These loans may also be backed by export or buyer credit guarantees provided by the governments of the countries involved.

[20] Drafts are not always required by a credit.

(b) Note Purchases / Forfaiting

86. Financial entities can purchase promissory notes or bills of exchange issued by foreign buyers to exporters for the purchase of goods and services, freeing up cash for the exporter.

(c) Factoring

87. In international trade, factoring is the purchase or discounting of a foreign account receivable for cash at a discount from the face value. While factoring is primarily undertaken by non-bank financial entities, banks may participate in factoring if the exporter has obtained accounts receivable insurance that guarantees the liquidity of the accounts.

(d) Guarantees

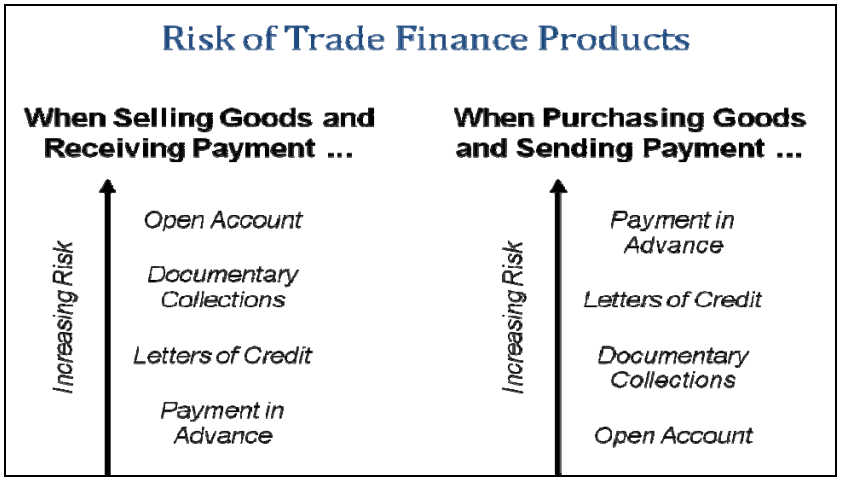
88. Guarantees are provided to or by financial institutions on behalf of exporters. Two popular types of export guarantees are pre-shipment and performance guarantees.

- *Pre-shipment Guarantees* encourage other financial institutions to advance pre-shipment loans to fund the upfront costs associated with an export contract.
- *Performance Guarantees* providing contract performance cover to buyers on behalf of the exporter.

89. It should be noted that both guarantees and standby letters of credit may be used in various ways to generate the purchase or sale of goods or services. In those cases many of the documents outlined in the steps above may or may not be utilised as part of the transaction.

Transaction risks for importers vs. exporters

90. The graphic below shows the different types of core trade finance products available, and positions each in terms of transaction risk, from the importer's and from the exporter's perspective. Importers and exporters consider these transactional risks in conducting legitimate trade transactions. The product choice will depend on the level of trust between the buyer and seller. Proliferators will also consider transactional risks when deciding how to sell/purchase and receive payment for/send payment for goods.



Source: Canada.

Risk Management and Customer Due Diligence (CDD)

91. All financial institutions involved in trade finance, no matter what their business line, have both commercial incentives and legal obligations to conduct CDD and potentially account monitoring. But the nature and depth of CDD undertaken, and how it is organised, can vary significantly between financial institutions, from transaction to transaction and based on the regulations in the local jurisdiction.

92. Some elements of CDD are universal: CDD processes include the identification and, in a risk-based manner, the verification of the identity of customers and reasonable measures to identify and verify the identity of beneficial owners, obtaining information on the purposes and intended nature of the business relationships and conducting ongoing due diligence. Of these components, the identification and verification of identity of customers are requirements that need to be completed in all situations.

93. The implementation of other components of CDD is variable, depending on the risks associated with the transaction and the legal requirements in the jurisdictions involved. A reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanism used to meet these standards.[21] The CDD process that a financial institution will perform before they act or an international trade transaction will be dependent upon a number of factors, these include:

- Specific regulatory requirements or guidance to which it is subject.
- The role which it will be required to perform in the transaction.[22]
- The institution's own exposure to financial or reputational risk through the transaction.
- Its assessment of the risk posed by the country in which the instructing party is based or operates.
- Its assessment of the risk nature of the underlying trade business (*i.e.* the goods, products or services being traded.).
- Whether any other higher risk parties appear to be involved as owners or intermediaries.

94. Appropriate CDD measures, relying in particular the factors above, are a critical first step for a financial institution to mitigate the risk of proliferation financing.[23]

95. Where the financial institution is granting any form of credit to the party from whom instructions are expected, then more extensive information would be requested as part of the CDD process, focused particularly on the client's financial standing, credit risk, and ability to repay. Equally where the financial institution assesses a customer to be higher risk then it may well employ "enhanced CDD" to the extent that a risk-based approach is allowed by the relevant regulatory authority.

---

21 FATF (2007)

22 In a letter of credit transaction, for example, financial institutions view different parties in the transaction as their customers for CDD purposes. As an issuing bank the applicant of the credit will be their customer, as an advising, nominating or confirming bank the issuing bank will be their customer. In some cases the beneficiary of a credit may be the customer of the advising, nominated or confirming bank and they may have done CDD on that beneficiary, however in most transactions the banks look to the issuing bank as their customer.

23 Customer Due Diligence is, depending on the type of internal organisation, conducted at the relationship management area rather than in the trade operations. This area may be a specific relationship manager, a relationship management group, a client coverage area, a compliance group or other area designated by the bank. Depending on the bank's internal policies and procedures the actual point of review, investigation, notification, determination, decision or reporting may vary.

96. Each financial institution has its own organisational structure for conducting CDD, an element of which may include outsourcing to employees that are located in different countries and undertake transactions that are not local to them. The same obligations for CDD apply no matter what arrangements are in place for implementing them.

Correspondent Banks

97. In the context of trade finance it is important to note that no one financial institution will undertake all aspects of CDD related to a specific transaction; and as discussed, different financial institutions will be responsible for individual elements depending on their role.

98. Since financial institutions in foreign countries do not necessarily have a presence in all countries or a relationship with all financial institutions, financial institutions are sometimes used as correspondents in the payment chain. Payment transactions are ordered in a foreign country, transit through one or more financial institutions and finally are received by the beneficiary located in a second foreign country. Such transactions may also occur when designated financial institutions in a country are prohibited from conducting financial transactions with institutions from another country, and therefore a correspondent financial institution in a third country is used as an intermediary.

99. With banks undertaking international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence, correspondent banks must rely on the respondent bank's due diligence and monitoring controls. However, a financial institution would not normally initiate a transaction on behalf of a party it does not know.

100. A primary objective for any financial institution when agreeing to accept instructions from a correspondent will be to ensure that the correspondent conducts satisfactory CDD on its own customers. Establishing a correspondent relationship might involve an understanding of the customer and documenting that the associated CDD obligations are undertaken.

101. As part of due diligence which is performed on a potential correspondent it is critical for the financial institution to agree and establish the types of accounts, if any, they will operate and the means of exchanging authenticated (bank to bank) messages. These mechanics are necessary for the handling of international trade transactions.

102. Although many financial institutions have procedures to ensure that the respondent institution's controls are adequate to mitigate the risk of money laundering and terrorist financing,[24] most do not specifically assess whether a respondent institution has adequate controls to detect and prevent proliferation financing. Such assessments may rely on information that is not currently reviewed as part of correspondent banking procedures[25], such as information related to a respondent financial institution's trade finance controls or its association with a state proliferator.

103. For more information in the risks related to money laundering and terrorist financing by correspondent banking, see the FATF Report on Money Laundering Typologies 2001-02.

Reviewing and monitoring transactions

104. Financial institutions manage a wide range of risks in the processing of international trade business. In practice risk management will normally include credit risk, including cross border or country risk, and the operational risk. Exposure to money laundering and terrorist financing form part

[24] For more information in the risks related to money laundering and terrorist financing by correspondent banking, see FATF (2002).

[25] Customer Due Diligence for correspondent banks is usually conducted in a centralised relationship management area within financial institutions. This area may be a specific relationship manager, a relationship management group, a client coverage area, a compliance group or other area designated by the bank.

of the overall risk management process. Such risk management processes will influence what arrangements are in place for reviewing documents and monitoring transactions.

105. If there is potential exposure to proliferation financing, financial institutions consider whether parties involved in payments are named in UN or relevant local sanctions lists or are considered to pose other risks. For example, if the transaction is subject to any export licensing requirements or trade embargoes.

106. All financial institutions are expected to have a form of financial transaction monitoring in place. The form of monitoring varies between (and within) institutions, including automated or manual checking, or a mixture of both, in order to monitor the transactions handled. This may involve reviewing customers' accounts or patterns of activity.

107. The information presented to a financial institution will vary according to the nature and complexity of the transaction. The extent to which this information needs to be verified will also vary. In general a financial institution will normally examine trade instructions received to establish whether:

- They have CDD on the instructing party;
- The instruction is consistent with what would normally be expected from the instructing party.

108. Financial institutions will also check the documents presented to them in accordance with relevant International Chamber of Commerce (ICC) rules and accepted banking practice. Furthermore, where letters of credit are concerned, the vast majority of transactions will be subject to commercial expectations and ICC standards which determine the time allowed for processing the various stages during the lifespan of the letter of credit.

109. It should be noted that in processing trade finance transactions, financial institutions deal with documents, not the physical goods to which they relate. Any physical inspection of goods will only occur in exceptional circumstances and would tend to relate to wider credit issues where the underlying goods are pledged as security. However, commercial parties to the underlying transaction may use other agencies to independently verify a particular shipment. Consequently inspection and verification measures in relation to physical goods are relatively rare as the vast majority of trade transactions are conducted legally between parties who willingly disclose all the information needed to conclude such transactions.

110. However, some existing transaction monitoring controls currently employed by financial institutions may result in the detection of proliferation finance. Financial institutions may currently detect transactions associated with proliferation activity by screening transactions against proliferation-related United Nations sanctions lists, such as the list of individuals and entities designated pursuant to S/RES/1737 (2006), or other local proliferation sanctions lists, to detect the presence of an individual or entity involved in proliferation in the transaction. In some cases, financial institutions may also attempt to verify whether a transaction is subject to any export licensing requirements or trade embargoes by requesting additional verification or documentation, such as export control licenses.

Identifying Suspicious Activity

111. There are several points in the trade finance cycle at which financial institutions could potentially detect suspicious activity if provided sufficient information by their customer and/ or relevant government authorities. For example, CDD processes can establish risks: whether a customer is a producer or buyer of goods or services which the institution regards as high risk, including ongoing monitoring of transactions, as described above, can also identify activity which may be intended to obscure the ultimate counterparties to the transaction or the eventual destination of goods.

If suspicious activity is suspected, the role of financial institutions is not to determine the underlying criminal activity; but to report suspicious activity in line with their domestic legal framework and relevant local regulations (including data privacy laws).

112. Financial institutions rely on export control regimes and customs authorities to police the activities of exporters which are its customers, in part as financial institutions are unlikely to have staff technically qualified to understand whether an apparently legitimate or innocent trade transaction is subject to such a control or whether in any event it is actually part of a proliferation finance scheme.

113. The ability of financial institutions to detect suspicious activity in their trade finance operations is constrained by several factors:

- The description of goods may be too vague and/or technical for a financial institution to determine if it is proliferation-sensitive or not.
- The fragmented nature of the trade cycle and the involvement of different financial institutions in a single transaction.
- The systems used to monitor transactions and volume of transactions will also influence the ability to review information and identify potential suspicious activity. Even where only a single financial institution is involved in a transaction, the organisational complexity of the institution may mean that no one individual examines all elements of CDD and monitoring associated with a transaction. This can make it difficult to identify complex or large-scale patterns which might indicate suspicious activity.
- The detection of fraud or money laundering by financial institutions is based on well-understood indicators and profiles, developed from a substantial case history. Proliferation financing has only recently garnered attention and consequently has not been incorporated into financial institutions' due diligence processes – whether through profiles or staff training programmes - to the same degree. Indicators or "red flags" invariably only become evident after the event when a transaction has already been completed.
- The availability of specific information regarding suspicious or high-risk entities is critical, as the factors noted above limit financial institutions' capacity to detect generic patterns associated with proliferation financing. Therefore, the ability of a financial institution to detect and identify potential proliferation financing is dependent on clear guidance or specific intelligence provided by authorities.

Money Services Businesses

114. Apart from supervised payment services, illegal, informal or registered money services businesses or alternative remittance systems (*e.g.* Hawalas) can also be used to transfer funds. Entities involved in proliferation financing activity may also use this sector if there is strong detection or monitoring measures in place for financial institutions in the formal sector.

Authorities relevant for export control

115. A jurisdiction's export control policy is usually implemented by a number of agencies that have varying responsibilities. The main authorities, which contribute to the implementation of the export control policy, are as follows:

- Licensing authorities
- Law enforcement and customs authorities
- Intelligence services (as a part of their general duties)

116. In accordance with their specific responsibilities, licensing authorities, law enforcement and customs authorities and intelligence services each play a major role in the prevention of proliferation. Licensing authorities decide whether the export of an item is subject to licensing or is exempt. They are also responsible for making licensing decisions – and for informing exporters of the decisions they have made. Normally, in adherence to their international obligations under relevant multilateral arrangements, jurisdictions will require an export licence application for controlled goods.

117. Items covered by national and international lists usually range from weapons, ammunition and related production facilities via material, plants and equipment for nuclear, biological and chemical purposes, high-grade materials, specific machine tools, electronic equipment, computers, telecommunications up to specific chemical units and chemicals. In addition to the licensing requirements for listed items, there are often licensing requirements for non-listed items depending on the use they may be put to. Experience shows that unlisted items are playing an increasing role in proliferation activities. Export control systems may incorporate "catch-all" clauses, to restrict trade in such items that in circumstances could be used for proliferation purposes. However, these catch-all clauses are usually only triggered when the destination and end-user is known to be of proliferation concern, unless there is evidence that the destination / end-user has established front companies elsewhere to try and circumvent controls. In cases concerning sensitive jurisdictions, technical assistance as well as the trafficking and brokering of items particularly from 3rd countries to those destinations may also be subject to additional controls.

118. National export control regimes usually provide that the exporter is liable for compliance with the restrictions and licensing requirements in force. Therefore, licensing authorities often reach out to industry in order to make them aware of their responsibilities. Ideally, licensing authorities and exporters work together to ensure compliance with this legislation.

119. Law enforcement and customs authorities monitor and control trade in order to detect deliberate offenders who illegally export or divert strategic proliferation-sensitive goods, software and technology. Law enforcement and customs authorities decide whether the exporter or importer wishing to export, import or transit their jurisdiction respects national and international regulations. Focus is most often placed on the verification of exports through selective risk-based examination. In the case of exports to jurisdictions of concern, efficient systems will often require all exports to be examined in this way. Surveillance procedures are used in the first instance to identify targets using documentation provided prior to export. The assessment of this information may lead to the targeting of particular shipments for physical examination. In some instances customs authorities may regularly decide to subject all cargo being shipped from a particular port or airport to such a destination to a physical examination.

120. Law enforcement and customs authorities are in a position to examine whether the description of the items in the export license match the items actually being exported. Customs authorities have the ability to physically inspect the goods, use their expertise and that of others within government with specialist knowledge of dual-use and other proliferation sensitive goods, to decide if export control requirements have been met.

121. If available, an intelligence service will provide specific information to enhance the monitoring by licensing and customs authorities. The intelligence function is a critical component for collecting, evaluating, collating, analysing and disseminating information on actual, suspected and potential export violations and trends. Intelligence is crucial in identifying suspected or known violators and ultimately unravelling complex networks. Intelligence is important in uncovering illegal procurement tactics such as diversion through false description of goods or the use of front companies. Intelligence is also used to detain and seize goods and may in certain circumstances be used by prosecutorial authorities. Provision of information on proliferation activities by intelligence is therefore a key element to prevent proliferation.

122. The exchange of information between customs and the wider export control enforcement community such as law enforcement, defense and export licensing authorities is imperative for an effective export control system. Licensing and customs authorities are in the best position to detect non-compliance with export control requirements, including criminal acts such as forgery of export documents and other related materials. However, financial information may provide another intelligence stream to supplement or reinforce existing channels in the fight against proliferation.

3. CASE STUDIES

123. The following 18 case studies illustrate some common techniques used by proliferators to transfer and export technology, goods, services or expertise that contribute to the proliferation of weapons of mass destruction.

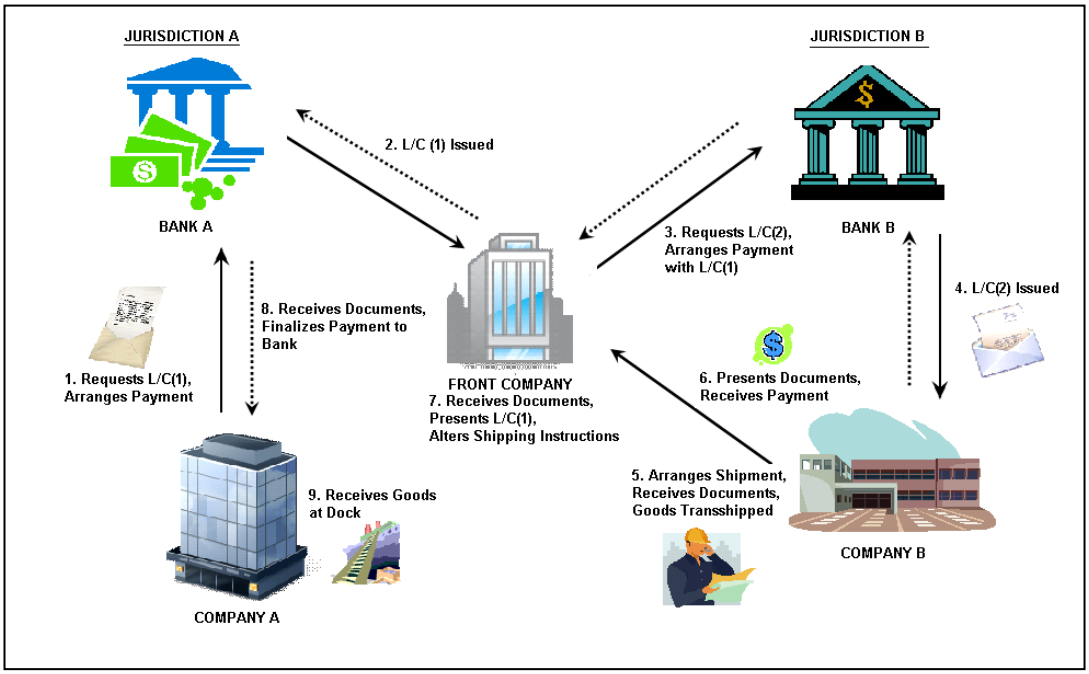
124. The cases also indicate that the international financial system is being used to facilitate proliferation. In many of these cases proliferators use letters of credit to settle trade in sensitive goods. In some there are more simple examples of wire transfers and large cash transactions that are used to move funds in efforts to facilitate proliferation. Annex 3 contains additional cases with no proven link to the financial sector, but that provide useful context.

125. While the majority of the cases mentioned in the report illustrate traditional means of trade financing such as letters of credit, there is no evidence that suggests that these financial instruments are more susceptible to potential abuse by proliferators. It would have been very difficult for the financial institution to detect proliferation financing based on evidence provided in the cases that illustrate links to the international financial system.

126. It is likely that proliferation background is more difficult to detect if other financial instruments, such as clean payments, are used. These cases studies describe features of the transactions, which were discovered through subsequent investigation, which would not at the time have provided a meaningful basis for financial institutions to report suspicions. They nevertheless can illuminate the financial features associated with the underlying acts of proliferation.

Cases involving letters of credit

Case 1: Letters of credit and front company



1. In **Jurisdiction A**, **Company A** requests that Bank A draw up Letter of Credit (1) and arranges payment for goods from a **Front Company**.
2. **Bank A** issues Line of Credit (1) to the **Front Company**.
3. The **Front company** then requests Letter of Credit (2) from Bank B in Jurisdiction B and arranges payment using Letter of Credit (1).
4. **Bank B** issues Letter of Credit (2) to Company B located in Jurisdiction B.
5. **Company B** arranges for shipment of goods to Front Company, arranges documents and transhipps goods.
6. **Company B** presents documents to **Bank B** and receives payment.
7. Front Company receives documents from **Bank B**, presents for Letter of Credit (1) and alters shipping instructions.
8. **Front Company** gets documents and finalizes payment to **Bank A**.
9. **Company A** receives goods at port.

Source: United States.

Case 2: Purchase of magnets through front companies and intermediaries

A proliferator set up front companies and used other intermediaries to purchase magnets that could be used for manufacturing centrifuge bearings.

False declaration
Front Company 1 signed documents with the foreign jurisdiction's manufacturing company concerning the manufacturing and trade of magnets, however, it was not declared in these documents, nor was it detected by authorities, that these components could be used to develop WMD.

Diversion
The magnets were transhipped through a neighbouring third jurisdiction to Front Company 2. This jurisdiction was typically used as a "turntable" for goods *i.e.* goods are imported and re-exported. The proliferator used an intermediary to arrange for the import and export of the magnets in this third jurisdiction. The intermediary had a sound understanding of the jurisdiction's export and commercial controls and used this knowledge to conceal the nature of the goods.

Using banks with poor AML/CFT controls
The intermediary also conducted financial transactions to settle trades. The intermediary had accounts with several banks in the third jurisdiction and used these banks to both finance the acquisition of goods and launder the illegal funds used for these transactions. A combination of cash and letters of credit were used to pay for the trade of the magnets, which totalled over 4 million USD.

Source: Gruselle, Bruno, (2007).

Case 3: The Thyratron case in Halmstad

In the spring of 1999 the Swedish Customs found out that a person (P) in Halmstad, via a pizzeria, had exported a thyratron to Iran that was classified as a strategic product and therefore was subject to export control. After an audit and interview with P, suspicions grew that it was a question of smuggling.
A search was made in the apartment of P and a seizure of a thyratron was made at Arlanda Airport. It was on its way to a jurisdiction of proliferation concern. Earlier another thyratron was already exported.
P stated that he had been contacted by his cousin in the jurisdiction of proliferation concern in the spring of 1998 who worked at a university in that jurisdiction. The cousin wanted P to get a thyratron to the university. The producer in the United States directed P to the branch in Sweden. P stated he would use it as a degree project at a Swedish university. He forged an end user statement in order to buy the thyratron.

P paid the company 22 000 SEK and delivered the product to Halmstad. P contacted a forwarding company in order for them to export the thyratron to a university in the jurisdiction of proliferation concern. P wrote a pro forma invoice in the name of the pizzeria. The buyer was the university in the jurisdiction of concern. The thyratron was then exported.

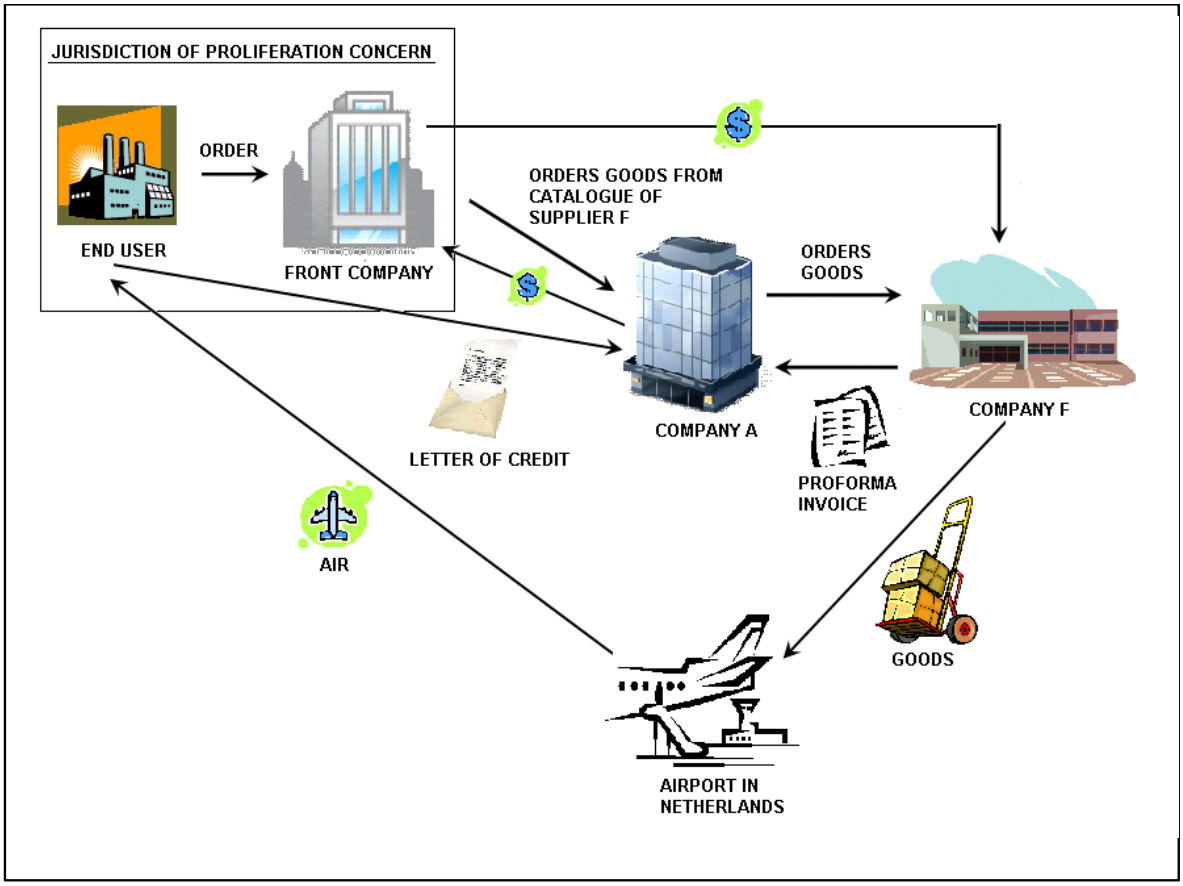
In November 1998 P ordered one more thyratron after an order from another university in the jurisdiction of concern. P paid the delivery and in 27 May 1999 the thyratron was delivered to P in Halmstad.

The forwarding company got an assignment to send it to the jurisdiction of concern. The product was not exported because P had not paid the forwarding company for the cost of the freight terminal. P had the impression that Iran Air would once again be responsible for all expenses like last time.

During the preliminary investigation the Swedish Customs found documents like dispatch notes for payment from abroad, inter alia, from the jurisdiction of proliferation concern.

Source: Sweden.

Case 4: Letter of credit and front company



A **Front Company** in a Middle-Eastern jurisdiction of proliferation concern, used the following method in order to obtain goods. The **Front Company** represents several large companies located in the jurisdiction of concern that are also established in Europe and other Western countries. The **Front Company** stands surety for the delivery of the needed goods to the companies in the jurisdiction of concern and executes eventual after sales services. The **Front Company** has the first contact with the true **End User** in the jurisdiction of concern.

The **End Users** order the needed goods from the **Front Company**. The **Front Company** orders the goods of the different Western companies from " **A**", that is to say, only on the basis of the article numbers in the catalogue and informs "**A**" about the supplier the goods have to be bought from. At request a L/C is opened in favour of "**A**". It also happens that "**A**" itself has to look for a supplier on the basis of an article number or article description. This happened worldwide. "**A**" orders the goods after having received the order (pro-forma invoice) from **F** and the L/C from the Middle Eastern client or end user. The goods that were bought outside the Netherlands came in transit to the airport of Schiphol and were delivered at a forwarding agent. The goods were sent from Schiphol airport to the jurisdiction of concern. "**A**" did not see the goods itself.

"**A**" placed the payment received from the end users through the L/C at the disposal of **the Front Company** by means of a bank account with a Dutch bank and after deduction of a commission. The suppliers were paid by the **Front Company**.

Source: The Netherlands.

Cases 5 to 8: State-owned entities

Three known instances of procurement for WMD programmes routed through state-owned banks whose overseas branches and correspondent banking partners facilitate business with foreign suppliers:

Case 5: Company A, a well-known front company for one of the entities responsible for country Z's ballistic missile programme, in order to buy 'special items' from country X, opened a Letter of Credit at a branch of a state-owned bank in Z's capital. The London branch of the same state-owned bank was named as the Advising Bank and in due course transferred payment to the supplier of the 'special items'.

Case 6: A branch of the same state-owned bank in another European capital was instructed to transfer over $100,000 to the account of a company in country U, a near neighbour of Z and a known diversionary destination. The company is owned by a well-known procurement agent who asked for the money to be transferred to a specific UK bank in order to cover the purchase of goods associated with a Letter of Credit opened with a branch of the same state-owned bank in Z's capital.

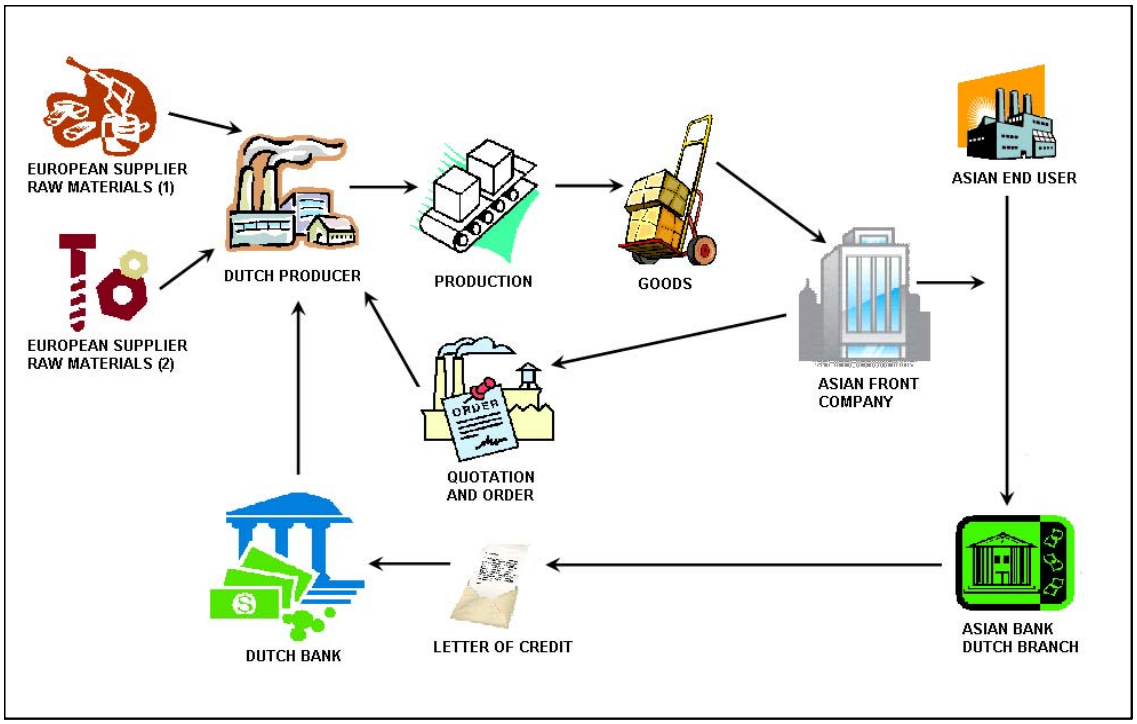
Case 7: In country Y, a state-owned bank known as the X Commercial Bank is known to have close relations with country Y's main arms exporters. In the past it has routed transactions through European banks. Recently it has sought correspondent bank relationships with several banks in a large Asian country, seeking to open Euro and US dollar accounts.

Use of a UK bank in a Diversionary Destination

Case 8: Trading company B in country Z deals in laboratory test-equipment for university and research centres and also for the energy sector. It is known to have procured dual-use items for country Z's WMD programmes.
Company B has bank accounts in a number of countries and has a UK account with a UK bank in country U, a known diversionary destination.

Source: United Kingdom.

Case 9: Infringement of export controls and Letter of Credit



This case concerns the infringement of export controls. Strategic goods were exported without the obligatory authorization. The Dutch producer was contacted by a Front Company, in an Asian jurisdiction of proliferation concern, to provide certain strategic goods, carbon fiber with special characteristics. The Dutch producer ordered the materials from two suppliers in other European countries. Payment took place through a Letter of Credit. The bank of the true Asian end user actually issued the letter of credit to the Dutch bank of the producer.

Finally the prosecutor decided to no longer pursue this suspect, since during the pre-trial the testimony of the expert stated that after the specific production performed by the Dutch producer, the end result of the carbon fibre no longer contained the characteristics for which it qualifies as a strategic good.

Source: The Netherlands.

Case 10: ASHER KARNI

Overview

Asher Karni was the principal in an import/export business known as Top-Cape Technology. In July 2003, agents from the U.S. Commerce Department (Commerce) and the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement learned that Karni was in the process of acquiring 200 triggered spark gaps from a company in Massachusetts and that he planned to have the triggered spark gaps sent to Top-Cape in South Africa, from where the items, at his instruction, would be re-exported to Pakistan. Triggered spark gaps are high-speed electrical switches that are capable of sending synchronized electronic pulses. They can be used as detonators of a nuclear device.

Investigation and outcome

U.S. export laws and regulations require the issuance of a license for the export of triggered spark gaps to Pakistan. At the request of investigating agents, the manufacturer agreed to disable the triggered spark gaps before they were shipped to Karni's company in South Africa through a broker.

In October 2003, Karni's company illegally sent the triggered spark gaps to Islamabad, Pakistan via Dubai, UAE. Karni was arrested on Jan. 1, 2004, in Denver, CO, when he arrived for a ski vacation. He was detained pending trial. In September 2004, Karni pled guilty and cooperated. Karni acted as a middle man for Khan, a Pakistani, in illegally shipping both triggered spark gaps and oscilloscopes to Pakistan. Khan was indicted in April 2005. Karni received credit for his cooperation and was sentenced to 36 months in prison in August 2005.

Financial elements

The triggered spark gaps shipment was financed via letter of credit opened by Khan at the National Bank of Pakistan with the Standard Bank of South Africa.

Source: United States.

Case 11: Thiodiglycol

US Immigration and Customs Enforcement, Office of Investigations, through its predecessor agency the United States Customs Service, conducted an investigation into the illegal export of thiodiglycol, which is a precursor for sulfur-containing blister agents found in Mustard Gas. Thiodiglycol is a Chemical Weapons Convention schedule 2 chemical used in the production of sulfur-based blister agents such as mustard gas.
http://en.wikipedia.org/wiki/List_of_Schedule_2_substances_%28CWC%29

The investigation had revealed that Alcolac International, a United States based company, was shipping large amounts of thiodiglycol out of the Baltimore Port of Entry to several transshipment countries with a final destination to Iran. During the investigation, agents encountered a large shipment of thiodiglycol with a declared final destination to a "Far East country." Agents substituted the chemical with water and tracked the shipment from the United States through two transshipment countries and ultimately to Iran.

The investigation led the agents to multiple bills of lading for shipments to other companies with one marked "Transshipping is allowed." A review of the financial documents and related bank records revealed multiple Alcolac Letters of Credit noting preference for immediate payment in cash. Agents also discovered that subjects attempted to open new accounts under shell companies in the US to facilitate the exportation through a letter of credit.

Alcolac International pled guilty to two counts related to the illegal export of thiodyglycol. As a result the company was fined $437,594. Several additional individuals who took part in the illegal exportation of thiodyglycol were also found guilty.

Source: United States.

Cases involving other payment methods such as wire transfers and cash transactions

127. The following cases show how proliferators use wire transfers and cash transactions to support their activities. Case 13 also provides an example where a proliferator under-valued shipment in efforts to disguise the true nature of the goods being transferred.

Case 12: Sponsoring of students by a known WMD procurement entity

Voluntary information received from a Canadian intelligence agency indicated that **Individual 1**'s education in Canada was sponsored by a known WMD procurement entity located in **Country X** and that **Individual 1** was possibly a procurement agent.

Analysis of FINTRAC's information revealed that **Company A**, located in **Country X**, sent Electronic Funds Transfers (EFTs) to **Individual 1** and three other individuals (**Individuals 2, 3 & 4**). For some of the EFTs, the transaction was noted to be for "cost of study". All EFTs were sent to personal bank accounts and totalled about $140,000 US.

Other than all receiving funds from **Company A**, no apparent connections between the four individuals were identified. **Individuals 1 & 2** were found to be located in two different Canadian provinces, while no address was found for either **Individual 3** or **Individual 4**.

During the same period, a Large Cash Transaction Report (LCTR) received from a depository financial institution indicated that **Individual 2** also deposited about $10,000 US into his/her personal account. The LCTR further indicated that **Individual 2** was a student.

It is unknown why **Company A** would be funding the education of these four individuals. However, the research field in which **Company A** was involved indicated a possible association to a WMD program. In addition, at the time, **Country X** was known to sponsor students who agreed to study overseas in science and engineering programs. It was suspected that **Country X**'s objectives were to gain knowledge and expertise in some areas that could be useful for its WMD program.

Source: Canada.

Case 13: AMLINK

Overview

R. David Hughes was the president of an Olympia, Washington-based company, AMLINK. AMLINK was a medical supply company, but was involved in export of commodities that did not match its business profile.

In June 1996, the U.S. Customs Service began an investigation of the exportation of nuclear power plant equipment by Hughes and AMLINK from the Port of Seattle to Cyprus. According to a confidential source, the nuclear power plan equipment was to be shipped from Cyprus to Iran via Bulgaria, in violation of the U.S. embargo on Iran.

Investigation details

The equipment in question was nuclear power plant equipment that had been purchased in an auction by a Washington company, LUCON. The origin of the equipment was a Washington-based power company that led a consortium in the 1970s to develop a nuclear power station in Burlington, Washington. The power plant was cancelled in 1983, and the equipment was sold. Hughes worked with another individual, a Lebanese national with permanent U.S. resident status, Habib T. Abi-Saad to purchase the equipment from LUCON, export it to Cyprus and attempt to find buyers for the equipment. Hughes used a freight-forwarding company to assist in arranging the shipment.

The equipment was transported in three shipments from Seattle in 1995, which transited Rotterdam, before arriving in Cyprus. Although the documentation regarding the shipment did not indicate it included nuclear equipment, Cypriot authorities who inspected the cargo determined that it was nuclear-related equipment. The equipment was controlled by the Nuclear Regulatory Commission and required a license to export. Hughes did not request or receive such a license. Further, documentation/bills of lading were marked “for re-export only,” but there was no end destination or consignee was provided and the exporter provided vague/incomplete information to the freight forwarder on commodities involved.

Hughes was indicted and convicted of export of nuclear equipment without a license.

Financial elements

Payment was made via wire transfer from Abi-Saad into Hughes U.S. bank account; Hughes then paid for the equipment with a cashier’s check. The declared value of the shipment was under-valued with ten containers being exported with a declared value at $20,000, even though it would cost $2,000 to ship an empty container out of the country.

Source: United States.

Case 14: Use of financial information in a case of an attempted procurement

Information sent to the Canadian FIU identified individuals and entities that were suspected of being involved in the procurement of technology that could be possibly used for WMD programs.

It was alleged that **Company 1**, located in Country Z, received a request from Foreign **Individual X** for price information regarding a magnetostrictive sensor instrument for guided wave research, and declared Foreign **Company X** as the end user. **Company 1** informed Foreign **Individual X** that it could not sell the equipment due to Country Z's export restrictions. The equipment utilizes wave propagation and acoustic emissions to detect defects in piping systems. It is not specifically export-controlled, however, according to its design engineers it could have both nuclear and military applications. The following day, **Company 1** received a similar request for the same equipment from **Individual A** as a representative of **Company A**, located in Canada.

Company 1 noticed that **Company A** was copying Foreign **Individual X** on a series of e-mail exchanges.

Foreign **Individual Y**, the head of Foreign **Company X**, had created **Company A** and was listed as its General Director, while other Foreign **Company X** personnel occupied other executive positions within **Company A**.

Financial Elements
Analysis of the Canadian FIU's information revealed that a short time after that inquiry by **Individual A**, Foreign **Company X** ordered EFTs totalling over $100,000 US for the benefit of **Company A** over a period of about two months. The total amount appeared to cover the controlled item price plus an additional amount, possibly a commission for **Company A**'s services.

A few weeks later, **Company A** ordered one EFT, which appeared to have been an initial deposit, for the benefit of **Company 1**. One month later, **Company A** ordered another EFT for the benefit of **Company 1**, which covered the balance of the guided wave equipment price.

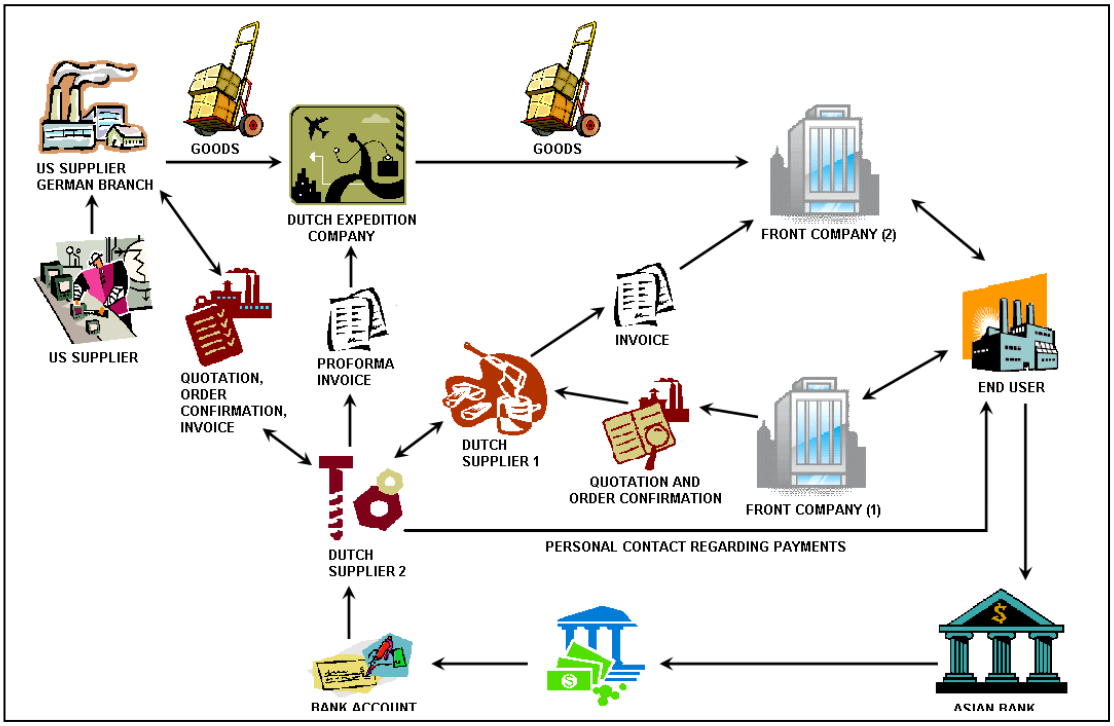
Investigation
An investigation revealed that Canadian **Company A** had been established by Foreign **Individual Y** specifically to market foundry software developed by Foreign **Company X.** Foreign **Individual X** is a member of the Research and Development department of Foreign **Company X** and was directing the purchase of the equipment through Canadian **Individual A**. Foreign **Company X** is a private research center and independent testing laboratory in the field of materials engineering, and is also involved in the development of materials engineering software for the foundry industry.

Individual A was described as "Management Executive", and operated **Company A** on behalf of Foreign **Individual Y**. This made it possible to distribute Foreign **Company X**'s foundry software to customers in Country Z as a means of circumventing its regulations.

Individual A and Foreign **Individual Y**, together with a third representative of Foreign **Company X**, were arrested while traveling to Country Z to receive training on the guided wave sensor.

Source: Canada.

Case 15: BANK BRANCHES



The case study clearly shows the difficulties in discerning the true purpose of trade when an authorization request is separated from the actual delivery of the goods.

The Dutch **Supplier 1** was contacted by two separate front companies, both located in an Asian jurisdiction of proliferation concern. The invoice was sent to one **Front Company A** in the jurisdiction of proliferation concern but the Dutch **Supplier 1** received the quotation and the actual confirmation of the order from another front company, **Front Company 2** (**Front company 1** and Dutch **Supplier 2** had personal contact with the **End User** in the jurisdiction of concern about the orders and payments.
This could be deducted from administrative information (emails and other documents) found at a research investigation at Dutch **Supplier 2**.

Dutch **Supplier 2** also contacted and confirmed that it could acquire goods form an additional supplier, **Supplier 3**, a branch located in Europe. The goods were then shipped directly by a regular Dutch expedition company to **Front Company 2**. The Dutch expedition company was unaware of the order confirmation and the invoice that was sent to the **US Supplier**, since it received a proforma invoice of Dutch **Supplier 2** directly.

The payments were received via wire transfers form the **End User's Bank** in the jurisdiction of concern, through a separate branch on the bank account of **Dutch Supplier 2**.

By using different companies (both in The Netherlands as in the jurisdiction of concern) that acted separately in different phases of the process, parties tried to disguise the actual circumstances of the trade transaction.

Source: The Netherlands.

Case 16: FRENCH CUSTOMS (EXAMPLE 1)

A French businessman is contacted by Pakistani nationals for the supply of dedicated electronic equipment for missile and/or drone tracking and guidance. He will acquire this equipment from an American intermediary, who will in turn order the components from an American manufacturer. Exportation of this sensitive equipment from the United States to France is authorised, provided that the latter country is the final destination. This operation is therefore subject to a prohibition on re-exportation from France.

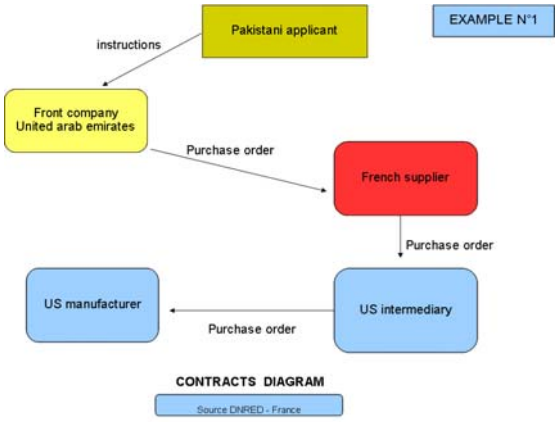
The equipment will not even be cleared from customs on arrival in France but remain in transit until immediate re-exportation to the United Arab Emirates, destined for a local front company acting on behalf of the Pakistani principal, which is affiliated with the Department of Defence (DoD) in Islamabad.

Contracts

A Pakistani purchasing network operating on European territory contacts a French industrialist to acquire electronic components that could be incorporated into tracking – ballistic control equipment for missiles or drones.

The French industrialist, who does not carry such equipment, contacts an American intermediary, which in turn places an order with an American electronic equipment manufacturer. On receipt, the intermediary decides to export the equipment to France, taking advantage of an export authorisation subjected to a restrictive condition prohibiting re-exportation from France.

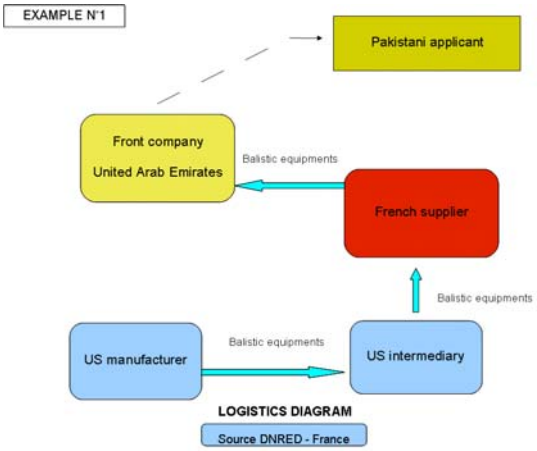
Meanwhile, a front company based in the United Arab Emirates, acting on behalf of the Pakistani principal linked with the Department of Defence, officially places an order with the French supplier.



Logistics

The equipment leaves the U.S. for France by express air freight.

It will not be cleared through customs in France. While in transit in Marseille, it is immediately re-exported to the front company in the United Arab Emirates, which assumedly then delivers the equipment to Pakistan.



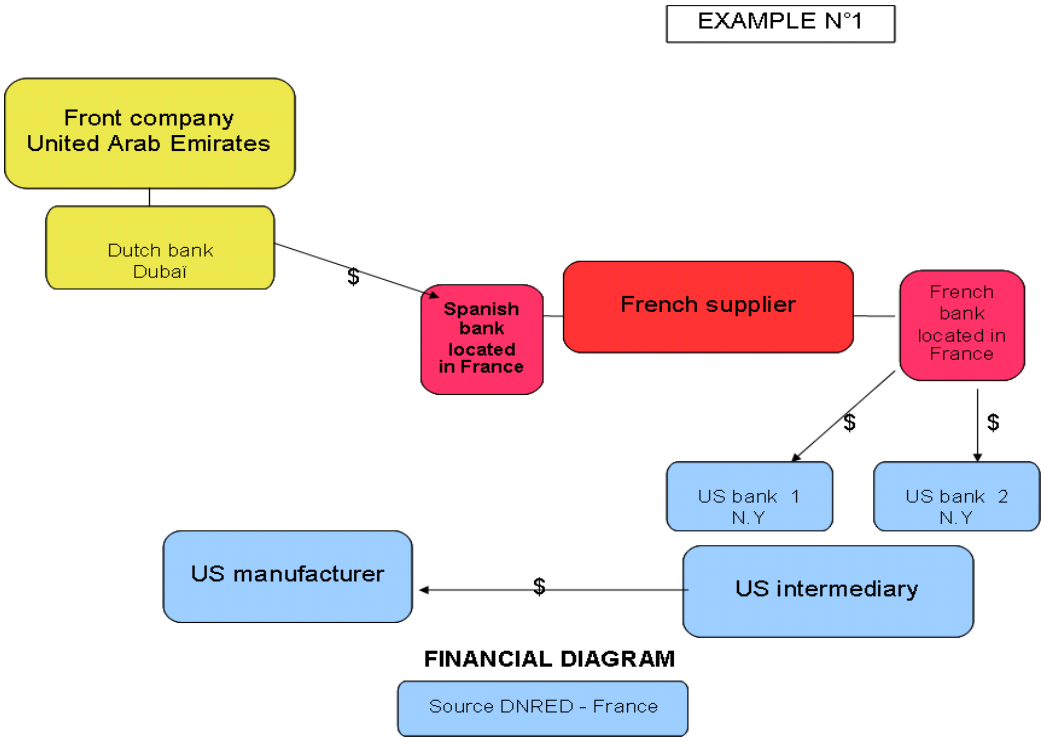
Case 16: (Cont'd)

Financial elements

This involves a direct financial transfer from Dubai (branch of a Dutch bank) to one of the French company's two banks (French branch of a Spanish banking group + branch of a French banking group).

One bank (branch of the Spanish bank) receives the money from Dubai and the other pays the American supplier, which itself has two banks, both domiciled in New York.

The transactions are split, both in France and in the U.S., between two banking institutions, seemingly unrelated because they belong to separate groups.



Source: France.

Case 17: FRENCH CUSTOMS (EXAMPLE 2)

Further to the action described in example 1, the Pakistani intermediaries acting on European territory established contact with a company specialised in designing and selling ballistic testing and programming equipment for missiles and drones.

This firm, very small (3 employees) yet capable of designing and producing high technology customised to satisfy its customers' needs, bought components from a Norwegian manufacturer specialising in the space industry (in which the firm had acquired financial interests) to then incorporate them into equipment exported to Pakistan. The shipments were split up to prevent inspection services from getting a comprehensive picture of the equipment (declared to Customs as electrical testing equipment), its characteristics and its sensitivity.

The equipment was exported without authorisation:

- either directly to Pakistan, destined for an import-export company fronting for the Department of Defence (DoD);
- or via an intermediary company based in the United Arab Emirates.

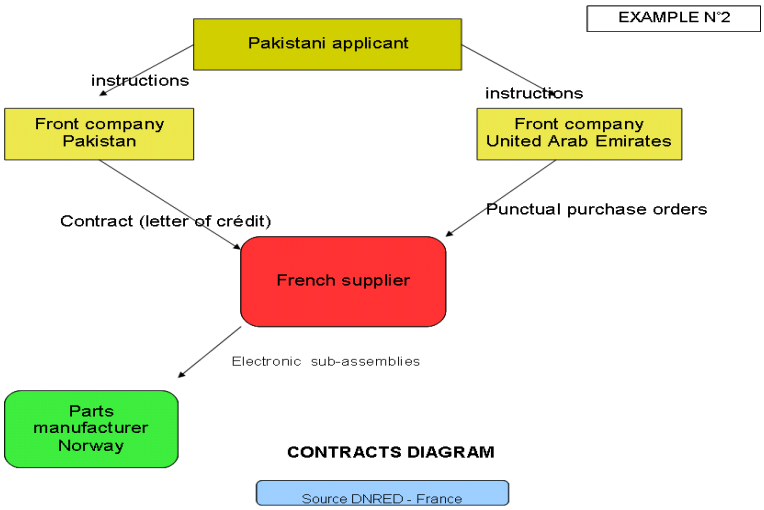
Searches were launched by French Customs at the firm's main office and at its employees' homes after an attempt to export one of the batches of equipment destined for Pakistan was intercepted at Roissy airport. These investigations confirmed the extreme sensitivity of all of the equipment (classified war materiel by the French Ministry of Defence) and the substantial involvement of the French company's director in the operations of the Pakistani military-industrial complex. The French company was declared dormant by its director. A claim was lodged by French Customs with French judicial authorities.

Contracts

The same Pakistani purchasing network (as in example 1), probably hoping to diversify and secure its supply sources in Europe, contacts a French businessman at the head of a small technological innovation firm (three employees) specialising in tracking and fire control equipment (missiles, drones). A contract is concluded concerning a complete calibration and guidance system for drones.

This project is divided into two separate but complementary orders. A first order is placed by a company based in Pakistan (55% of the system). A contract and letter of credit are drawn up for this order. The other part of the contract (45%) will be fulfilled through a succession of single orders by a front company based in the United Arab Emirates.

The two companies (Pakistan and UAE) both act on behalf of the same principal, i.e. Pakistan's Department of Defence (DoD). Down the line, the French integrator will procure part of the components required to develop the system from a Norwegian manufacturer which specialises in aeronautics and space and supplies the Norwegian army. The French integrator secures this procurement by taking a share in the Norwegian supplier's capital.

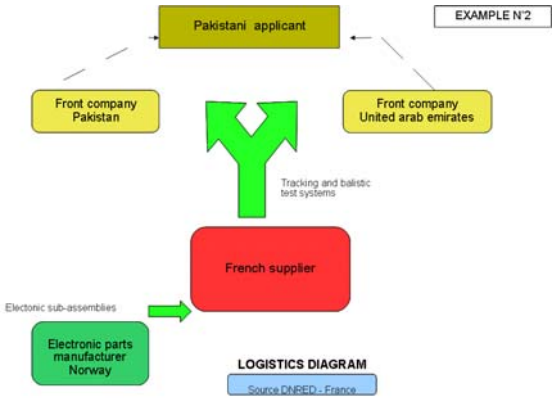


Case 17: (Cont'd)

Logistics

Upstream, the Norwegian manufacturer delivers its electronic subsystems to its French customer, which exports them directly in its name, one part to Pakistan and the other to the United Arab Emirates.

It is worth pointing out that, as is generally the case in such affairs, the real nature of the goods and their sensitivity were obscured by the innocuous-looking commercial wording of the customs declaration (e.g. electrical equipment).

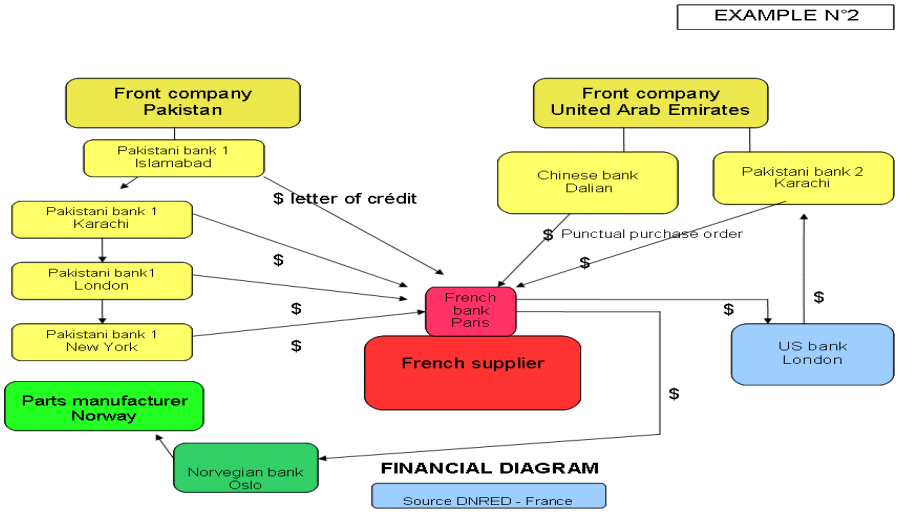


Financial elements

The financial diagram is highly instructive, because it shows the range of financing possibilities behind an act of organised proliferation. The Pakistani principal will go through two separate financing networks: 1) (right-hand side of the diagram) One network will put money into its front company in the United Arab Emirates and funnel the payments for single orders through a Chinese or Pakistani bank. Interestingly, the Pakistani customer indicates to the French seller that an American bank in London is to receive the kickback payments; and 2) (left-hand side of the diagram) The Pakistani buyer will use the letters of credit destined for a single French bank, where the French seller has domiciled its accounts.

These letters of credit will transit through four branches of the same Pakistani banking group (other that the one used by the front company in the United Arab Emirates) located in Islamabad, Karachi, London and New York, respectively.

The advantage of this scheme divided into two distinct parts is that the left hand doesn't know what the right hand is doing. However, all of the operations (left hand and right hand) were linked to a single French bank, a linkage that facilitated the French Customs' investigations. In addition, this French bank effected the payment of the electronic component orders placed with the Norwegian manufacturer via a Norwegian bank in Oslo.



Source: France.

Case 18: FRENCH CUSTOMS (EXAMPLE 3)

Information passed on by a French intelligence service reported visits by interns of country A to the main office of a French company based near Paris. This extremely dynamic company was headed by an independent industrialist, also the director of another firm. The two companies specialised in designing and manufacturing very high-tech dedicated products for ballistic applications. Concerned here were calibration tables for missile guidance systems that only found their equivalent at a Swiss supplier and an American supplier. In other words, the French industrialist headed one of the three specialists world-wide in that area.

The following facts also attracted the service's attention:

- This equipment was systematically declared free for export (neither licence nor authorisation for war materiel exports) under such surprising customs descriptions as electrical cabinets or kinaesthetic apparatuses.
- The buyers of this equipment were located in Pakistan, in country A and in country B.

French customs officers conducted an "in the act" (*flagrant délit*) interception at Paris' Orly Airport, with the support of their specialised counter-proliferation intelligence and investigation service. A machine was seized for examination at the time of the attempted export. The examination immediately confirmed at a minimum the dual civil and military nature of the equipment, whose destination was a ballistics research institute located in country A.

The searches conducted on the company's premises revealed that:

- Several machines had been exported illegally to those sensitive countries, either directly by one of the two French industrialist's companies or through the intermediary of a front company that received a commission for appearing to be the official seller of certain machines destined for various institutes of country A. The front company was also mentioned on the contracts, the letters of credit and the customs export declarations, whereas everything had been negotiated and organised by the French industrialist.
- Analysis of the equipment's technical characteristics found that it classified either as war materiel (therefore subject to a war materiel export authorisation) or as a product on the list of dual-use items (export licence - category 2B1 of the European Union's Community regime regulation).
- Hearings of the implicated companies' executives underlined the French industrialist's deliberate intention of circumventing existing export restrictions for his sensitive goods, whose strategic and military nature he knew perfectly well. In view of the potential buyers of the equipment, the industrialist knew that he could not obtain the necessary authorisations from French authorities. That was why the equipment was falsely declared in customs at exportation and why a front company in France was used in order to mask the real seller.
- As for the financial side of these sales, apart from the country A or Pakistani buyers' direct payments to the industrialist's companies by conventional letter of credit, most of the transactions were effected via the front company, the intermediary through whose accounts the money merely passed before the total, after an average 3% commission was skimmed off, was paid into the industrialist's companies' various accounts and then finally transferred to a financial structure belonging to the industrialist.

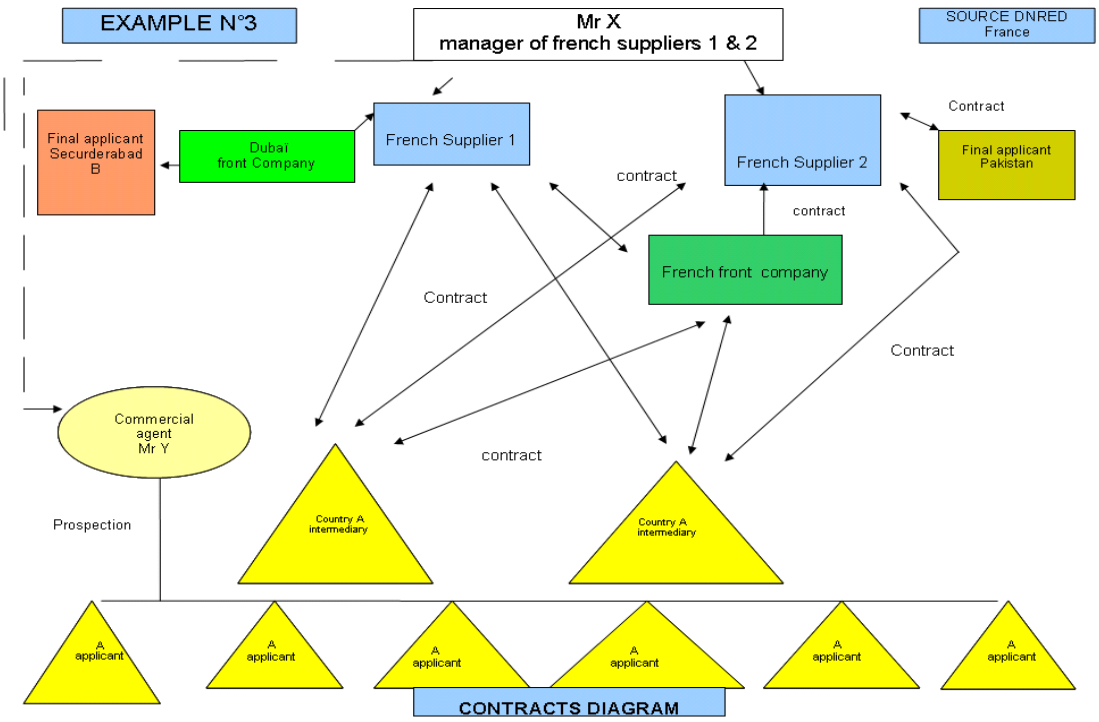
Case 18: (Cont'd)

Contracts

A French industrialist decides to set up business in at-risk countries – Iran, Pakistan, country A and country B – for which he knew he could not obtain the French authorities' authorisation to export sensitive equipment.

The investigation uncovered two kinds of commercial relations: 1) sales contracts entered into directly, with no intermediary (diagram upper right: Pakistani contract); or 2) contracts via various types of intermediaries:

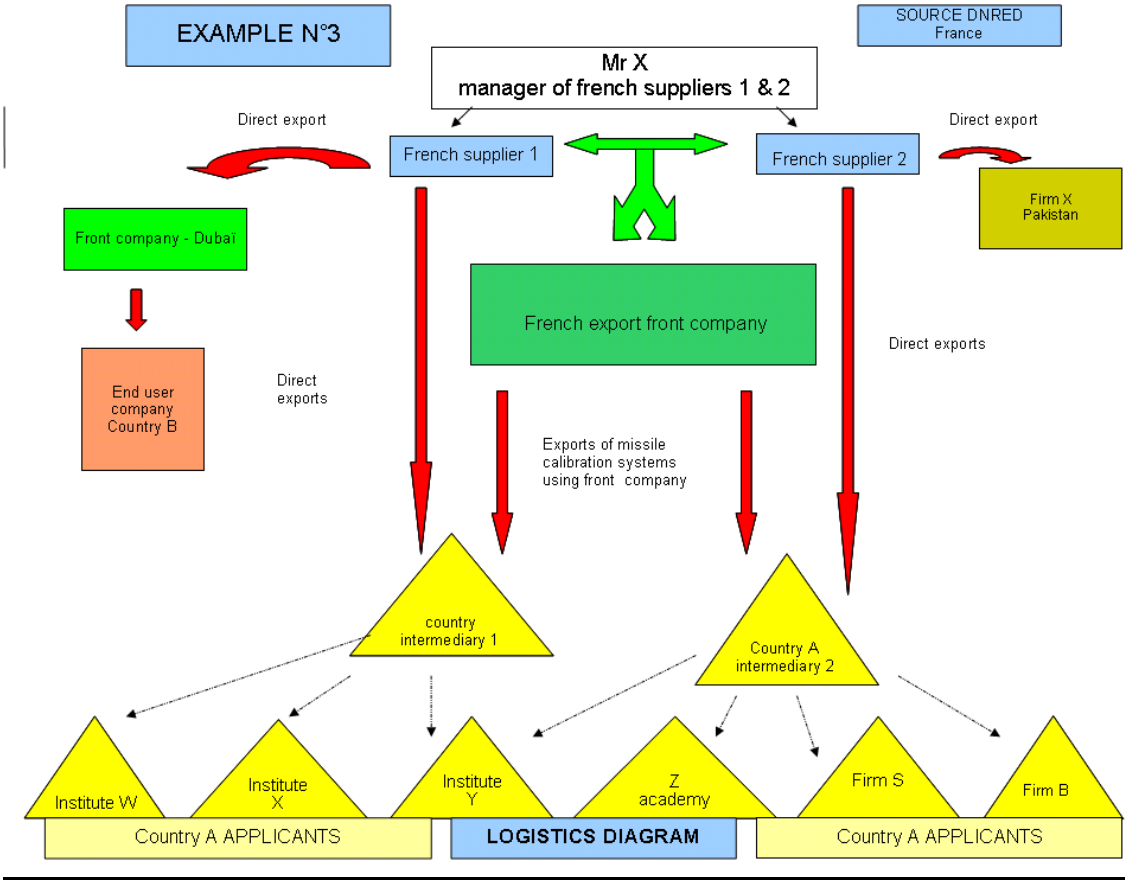
- Contracts via a commercial agent of country A canvassing the end users.
- Contracts via intermediary companies of country A disguising the real end customer (country A intermediaries diagram).
- Lastly, the most complex variant: use of a buffer company in France (French chain company diagram) to substitute for the industrialist and his company as the declared exporter of the sensitive goods.
- Another interesting point: a one-shot circuit for a B customer via a front company in the United Arab Emirates (diagram upper left).



Case 18: (Cont'd)

Logistics

The logistics diagram mirrors the contracts diagram. Direct exports by the companies controlled by the French industrialist to Pakistan and the United Arab Emirates, as well as to two A trading groups (intermediaries), responsible for forwarding the equipment to the final customers. The main exportation scheme used passes through a French front company mentioned on the customs declarations as the official exporter.



Case 18: (Cont'd)

Financial elements

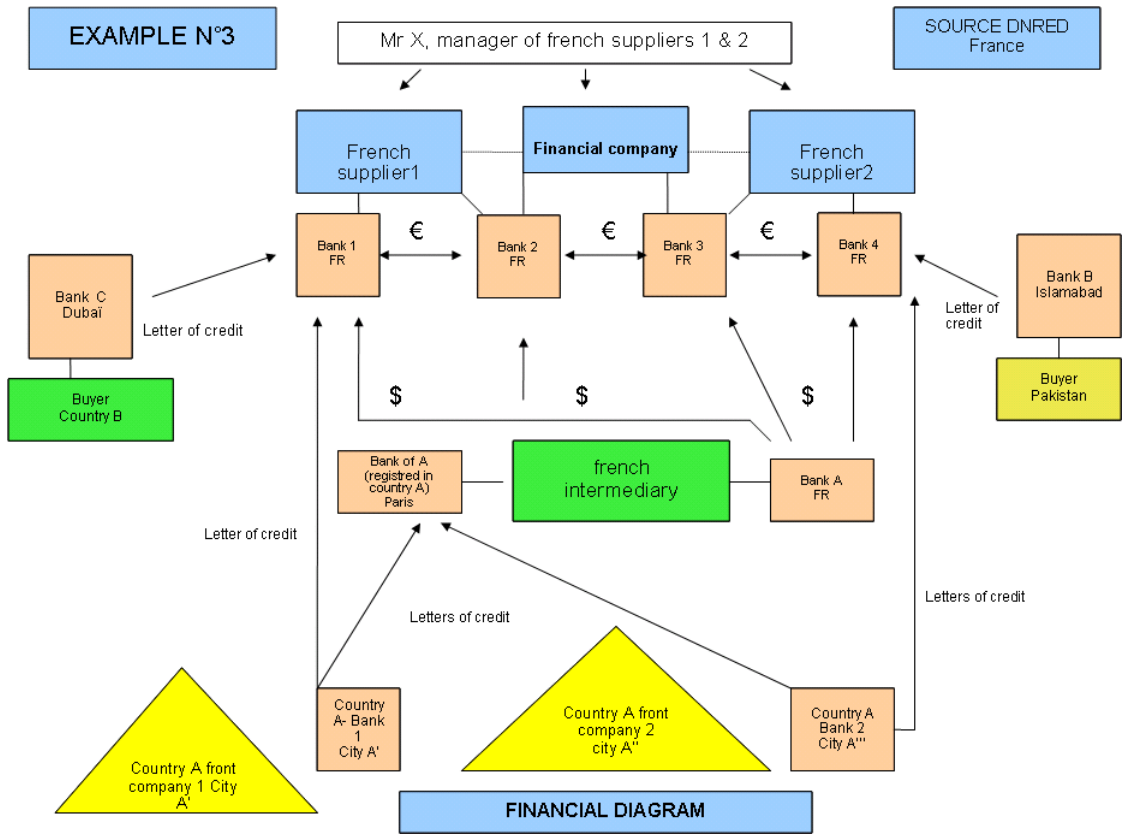
The financial diagram is highly enlightening as to the "left hand/right hand" model, in which the left hand doesn't know what the right hand is doing.

In general, it operates by letters of credit opened:

- Either directly by the foreign customer – Pakistani via an Islamabad bank or B using a Dubai bank – in the French companies' favour (suppliers 1 & 2).
- Or by A intermediaries in favour of the French front company (French chain company).

For the A operations, all of the letters of credit for the French front company are opened by two A banks at the Bank of A in Paris. This establishment then has those sums transit through a merchant bank in Paris, after skimming off an average 3% commission. The merchant bank, following instructions from the industrialist who organised the fraud, then transfers the sums to one or the other of his firms (suppliers 1 & 2), through one of their banks (four in all).

Even more interesting, the French industrialist had set up a financial structure (company) in the Paris area, totally independent of his companies, through which he could recycle that money as he wished, to his personal benefit.



Source: France.

4. COUNTER PROLIFERATION PURSUANT TO S/RES/1540 (2004)

128. S/RES/1540 (2004) was adopted unanimously on April 28, 2004 under Chapter VII of the UN Charter, with its objectives reiterated in S/RES/1673 (2006).

129. The resolution is the first international instrument to deal with the non-proliferation of all classes of WMD, their means of delivery and related materials in an integrated manner, and is the first international instrument to prohibit facilitating proliferation via financing. Operative Paragraph (OP) 5 of S/RES/1540 (2004) states that none of its obligations shall be interpreted to conflict with existing treaties. Annex 4 has a description of the most important conventions and other initiatives.

The key requirements of S/RES/1540 (2004)

130. S/RES/1540 (2004) represents the first time that the Security Council adopted a Resolution that broadly addresses the issue of WMD proliferation.

131. S/RES/1540 (2004) obligates States to take a wide range of actions to prevent and counter the proliferation of WMD. The main requirements of S/RES/1540 (2004) are found in OPs 1 to 3.[26] While those paragraphs set out multiple broad obligations, they are not prescriptive in nature, States are required to determine how best to implement the requirements of the Resolution, in accordance with their domestic laws and regulations and consistent with international law.

132. OP 1 prohibits States from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery.

133. OP 2 requires States to "adopt and enforce appropriate effective laws which prohibit any non-State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them". Of particular importance for the FATF's consideration, States must have in place prohibitions which address WMD proliferation financing activity.

134. OP 3 requires that States establish and enforce effective domestic controls to prevent WMD proliferation, including accountancy and physical protection over related materials, border controls, brokering controls, measures to prevent illicit trafficking, and export controls (including controls over transshipment and re-export, as well as end-user verification). In terms of proliferation financing, it is important to note that OP3 also requires that States put in place controls on providing funds and services related to the export of WMD-related materials, such as financing.

135. OP 8(d). asks jurisdictions to work with industry and the public on their legal obligations under laws implementing S/RES/1540 (2004). This requirement enhances the effectiveness of measures that have been adopted.

---

[26] *Non-State actor*: individual or entity, not acting under the lawful authority of any State in conducting activities which come within the scope of this resolution.

Means of delivery: missiles, rockets and other unmanned systems capable of delivering nuclear, chemical, or biological weapons that are specially designed for such use.

Related materials: materials, equipment and technology covered by relevant multilateral treaties and arrangements, or included on national control lists, which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery.

5. KEY FINDINGS ON THE IMPLEMENTATION OF S/RES/1540 (2004)

136. Based on the survey[27] results and the findings of the 1540 Committee[28], the following information is useful in considering how jurisdictions are implementing their obligations pursuant to S/RES/1540 (2004).

Export controls

137. Export controls are a key feature of, and effective implementation is an essential first step to, countering proliferation. However, the 1540 Committee reported that only 80 jurisdictions had any export controls related to WMD-related items, and only 69 had associated penalty provisions, among nearly 130 States. However, every jurisdiction responded to the FATF survey as having an export control system and most reported as having specific dual-use legislation covering dual-use items and catch-all provisions covering goods known or suspected for WMD end-use but not listed as dual-use items under their export control system. Some jurisdictions have prohibited any support for the development of WMD, including prohibition on financing activities related to it. Annex 5 provides information on some elements that traditionally contribute to effective export controls. In general it does not appear from survey responses that any jurisdiction's export control regime imposes special obligations on financial institutions to detect proliferation financing, a conclusion that is supported by the findings of the 1540 Committee.

138. Reports to the 1540 Committee show that a number of jurisdictions worldwide have not yet implemented lists of controlled goods and end-user controls. A limited number of jurisdictions control the transit, trans-shipment, or re-export of WMD-related items; efficient control may be more difficult in free trade zones. Jurisdictions that responded to the survey indicated the importance of end-user controls, including the examination and verification of end-users by authorities using Embassy assistance, assurances by foreign governments, end-user certificates, international import certificates and pre-shipment audits. Most jurisdictions that responded to the survey use a coding system for controlled goods, including dual-use goods; however, the use of this system presupposes detailed technical knowledge which financial institutions do not poses.

Sanctioning proliferation activities

139. The survey results indicate that one jurisdiction has legislation containing provisions that specifically criminalise proliferation and financial assistance related to proliferation, and that most have taken significant action to implement specific proliferation legislation and controls. Most jurisdictions have not implemented legal provisions that criminalise proliferation financing, indicating in the survey response that specifically criminalisation of the activity of proliferation financing is already covered by complicity provisions in connection with provisions criminalising specific activities related to proliferation. Depending on the breadth of complicity provisions in a particular jurisdiction counter proliferation legal framework, additional legal provisions may be superfluous.

140. No jurisdiction reported any convictions or charges related to proliferation financing. All jurisdictions reported to have asset freeze requirements related to S/RES/1718 (2006) on North Korea and S/RES/1737/1747 (2006/07) on Iran. In addition, some reported having an ability to impose asset freezes for known proliferators beyond their implementation of these resolutions.

---

[27] A survey was sent to all jurisdictions on 1 October 2007 and this report reflects the responses of 20 jurisdictions.

[28] Countries must report on their implementation of S/RES/1540(2004) to the 1540 Committee. The 1540 Committee's report to the Security Council was based on answers from 129 States (136 by August 2007) and the EU. This report, along with country reports are published on the 1540 Committee's website *http://disarmament2.un.org/Committee1540*. A forthcoming report of the 1540 Committee is due by 31 July 2008.

141. While some jurisdictions consider anti-terrorism laws to be sufficient in satisfying their obligations to prohibit proliferation by non-state actors, it should be considered if such legislation is applicable in all cases. For example, the 1540 Committee identified that non-state actors may not necessarily proliferate for terrorist purposes, or their activities may not lead to facilitating a terrorist act[29].

142. The could also be issues concerning the applicability of money laundering legislation when proliferation financing is derived from legitimate sources and is not connected to the proceeds of crime. Terrorism financing legislation may not be applicable if the financing does not ultimately result in contributing to a terrorist act. Again, the 1540 Committee has expressed to the Security Council its concerns with regards to the use of AML/CFT legislation, that it may not be sufficient to fully implement OP 2 requirements[30].

143. The FATF survey indicated that few countries have taken measures to monitor the activities of trade intermediaries, for example trading companies, freight forwarders, etc. One jurisdiction reported having legislative measures against proliferation through brokering and transport. In this example, a broker must obtain a permit for the trade with goods that are or might be destined entirely or in part for the purpose of WMD. One jurisdiction reported that it requires customs brokers, depot and warehouse operators to be licensed by customs authorities. One jurisdiction reported that freight forwarders are subject to a license/registration system.

Enforcement

144. Effective implementation of S/RES/1540 (2004) requires a significant amount of public resources, and it appears that jurisdictions are implementing a legal framework to deter and detect proliferation. However, the effectiveness of enforcement measures may differ from jurisdiction to jurisdiction. In its report, the 1540 Committee identifies a number of issues, and provides its recommendations concerning effectively maintaining and enforcing: border controls; export controls; licensing; controls related to items and controls related to transactions.[31] Annex 6 provides a chart from the 1540 Committee report that indicates that while a number of jurisdictions are enacting the necessary legislation for border and export controls, fewer have implemented appropriate enforcement measures.

145. Survey responses varied concerning the methods used by authorities to address the risks of proliferators diverting goods to circumvent export controls. The most elaborate responses noted the following as key elements used by the responsible authorities for detecting/preventing diversion:

1) Risk assessment.
2) Intelligence and information sharing.
3) Follow-up procedures to ensure products arrived at declared destination.
4) Legislative authority to ask for additional verification measures from an exporter, *e.g.* the proof of delivery through providing documentary evidence.
5) Ad-hoc verification after delivery by competent authorities, *e.g.* to check if goods are used for the intended purpose.
6) Authorisation for export of dual-use goods is followed by a letter informing company about the obligation to immediately notify the competent authority if conditions for the authorisation change, including if the company receives new information about the end-use of the goods, the end-user or re-export of the product.

29 United Nations (2006), Paragraph 40
30 United Nations (2006), Paragraph 41
31 United Nations (2006), Paragraphs 85 to 105

Exchange of information and outreach to private sector

146. Jurisdictions reported that information on proliferation is generally shared among competent authorities both domestically and internationally but on a case-by-base basis. Little mention was given to proliferation financing. Confidential information (names etc.) is exchanged domestically between limited authorities dealing with counter-proliferation and internationally in counter-proliferation forums. Some information is only exchanged between intelligence services. The EU has a system which requires Member States to provide all other Member States with information on denials of export licenses for dual-use goods. As a rule, the private sector is not privy to this information.

147. The survey results indicate that many jurisdictions are disseminating information about export controls publicly. In general, red flag indicators and typologies for manufacturers and/or export control and customs authorities as well as official targets etc, if existent, may be publicly available. This may, in some jurisdictions, include "countries of concern". Some information concerning critical countries, end-users, intermediaries and brokers may be shared with export control authorities (and part of this may be shared with the private sector on a case by case basis) while some of it will only be known by intelligence services.

148. Several jurisdictions indicated that they issue guidance concerning UNSCR-targeted persons and entities and other general information (see publicly available information under export controls) and AML/CFT indicators relevant to proliferation financing, while one jurisdiction doubted in general whether AML/CFT indicators could help detect proliferation financing. One jurisdiction reported that it provides a programme of outreach awareness-raising exercises with the financial sector on issues relating to proliferation more generally. These include seminars that highlight the importance of export controls and the relevance of these to financial institutions.

149. Some jurisdictions also mentioned that transport documents could help detect diversion, including the implementation of a safeguard provision covering competent authorities to receive documentation for goods arriving at the stated place of end-use. Some indicated that information on controlled goods held by international control regimes could be useful information for financial institutions to screen transactions for possible proliferation financing.

Financial measures in more detail[32]

150. Many survey responses suggest that CDD requirements may be the most useful AML/CFT requirements in countering proliferation financing. Some mentioned suspicious transaction reporting systems could be useful, and others referred in addition to the following requirements:

1) Record-keeping requirements.
2) Correspondent banking controls.
3) Prohibition on shell banks.
4) Reporting of large cash transactions.
5) Reporting of electronic fund transfers.

151. One jurisdiction reported that its financial sector would need consolidated information on companies that were denied export licenses. Guidance could help the financial sector in identifying industries deemed high risk that are not self-evident in addition to considering where goods and financial transactions are destined. Additional information concerning high risk individuals, entities and jurisdictions can be very useful for financial institutions.

152. Screening customer databases against lists of names, knowledge of customers' trading activities and knowledge of products, if available, are trade finance controls that could be most useful

[32] The following relies solely on information derived from survey responses.

in detecting and deterring proliferation financing. A financial institution that has some knowledge of the controlled goods lists and export restrictions may be in a better position to request additional information such as export licences, and provide guidance to clients on more complex transactions of trade financing.

153. Under normal circumstances financial institutions do not have a detailed knowledge of the underlying commercial transaction associated with a financial transaction undertaken for a client, in particular where there is no detailed documentary evidence used in the transaction, such as a letter of credit.

154. No jurisdiction reported to have any specific proliferation financing reporting for financial institutions, but several jurisdictions mentioned that reporting is encouraged[33]. However, in addition to electronic fund transfer and large cash transaction reporting, several jurisdictions mentioned that information may be reported under the suspicious transaction reporting system.

155. Jurisdictions generally reported that financial information could help counter proliferation and proliferation financing and provide useful information to ongoing investigations. There was some indication that information on financial aspects has proven to be useful in investigations on the infringement of export controls, and in one example the investigating authority will focus on financial aspects of trade to verify end-use and the true nature of the good. There was some indication of reports having been received by a financial intelligence unit (FIU) concerning entities and/or individuals suspected of being involved in proliferation financing activities. There was some indication that a financial audit had assisted in determining the extent of procurement of non-WMD controlled items and the involvement of others in the supply of dual-use goods.

156. Jurisdictions indicated that, in general, the following types of financial information could be useful to help detect diversion:

1) Information in any associated letter of credit.
2) All information on type of payment (letter of credit, wire transfers).
3) Information on financial transfers associated with commercial transactions, including specific information on parties to the transaction.

6. ISSUES FOR CONSIDERATION

157. The following section addresses the third objective, of the report: to identify measures (*e.g.* criminalisation measures, broader sanctions, activity-based financial prohibitions or controls or examining the use of financial intelligence) that could be considered in combating WMD proliferation finance within the framework of existing UNSCRs, such as S/RES/1540 (2004).

158. This study explains that proliferation financing poses a real and ongoing threat to the international financial system. Proliferators are using trade finance and other bank products to finance trade in proliferation sensitive items. However, proliferators use a variety of techniques, which are described in the report, to hide their true identities and their involvement in proliferation, as well as the true end-use of an item or an item's true end-user. Jurisdictions and financial institutions may remain vulnerable if these risks are not adequately considered.

159. The issues for further consideration by the FATF are presented along four broad categories: *i)* legal systems; *ii)* preventative measures; *iii)* awareness raising; and *iv)* investigations.

160. The analysis and observations contained in previous sections of this report suggests that financial measures could help in overall counter proliferation efforts, but the benefit of these measures

[33] Jurisdictions do require financial institutions to report on targeted financial sanctions pursuant to S/RES/1718(2006), S/RES/1737(2006) and S/RES/1747(2007).

will be very limited if more traditional counter proliferation measures are not effectively implemented and enforced. Effective proliferation financing prohibitions is one of several important elements that contribute to a jurisdiction's effective and comprehensive counter proliferation regime.

161. However, it is important to note that without a thorough implementation of controls to prevent the transfer and export of technology, goods, services or expertise, proliferation financing will be difficult to prevent and financial measures would not be useful.

Legal systems

162. S/RES/1540 requires jurisdictions to prohibit proliferation financing.

- There is limited evidence that jurisdictions have taken additional measures to criminalise proliferation and proliferation financing since the adoption of S/RES/1540 (2004).
- Most jurisdictions rely on complicity provisions and other provisions, such as terrorism financing provisions, to prohibit proliferation financing.
- There may be value in explicit criminalisation, including to:
  - Clarify the obligations on firms and financial institutions to be vigilant to proliferation and proliferation financing.
  - Enhance enforcement against proliferation and proliferation financing, including by establishing appropriate penalties.
  - Address financial activities not otherwise covered by export controls.
  - Provide a basis for financial institutions to report, when necessary, financial information related to proliferation financing to an appropriate competent authority within the domestic legal framework.
  - Provide a basis for competent authorities to receive, analyse and share financial information related to proliferation financing.
  - Properly cover intermediary activities, *i.e.* brokers.

163. Some jurisdictions are using targeted financial sanctions to prohibit proliferation financing, however most do not. There may be value to measures that create a domestic legal authority and capacity to implement targeted financial sanctions against individuals, entities and jurisdictions involved in proliferation financing. Such measures can serve to:

- Deprive proliferators of their assets and limit their access to the global financial system.
- Disrupt proliferation networks by publicly exposing designated individuals and entities.
- Provide detailed identifier information on designated proliferators, front companies and other associates, which could be used by financial institutions to effectively detect and prevent proliferation financing.

164. However, the use of targeted financial sanctions against proliferation financing has limitations. Automatic and manual screening through name based designation requires adequate and up-to-date identifier information for designated individuals and entities. This can be challenging for jurisdictions, which can result in false positives and failure to capture individuals and entities working on behalf of designated entities, or designated entities who have changed their names or other identifying information.

Awareness

165. While proliferation networks, including financing arrangements, use creative schemes to exploit unwitting actors, lack of awareness of proliferation and proliferation financing could contribute to the problem.

166. The majority of private sector entities do not knowingly engage in proliferation, want to be good corporate citizens and do not want to be involved in illicit activities. They avoid risks to their reputation and avoid having their assets unknowingly involved in proliferation.

167. Outreach by government to producers, sellers, transporters etc. on proliferation risks is critical, and already takes place to a high degree in many countries.

168. Outreach to the financial sector on proliferation financing risks does not take place to the same degree. When considering if and to what extent measures should be taken the nature of the services provided by the financial sector and the ability to detect proliferation finance must be taken into account.

169. Awareness-raising with authorities and persons/companies/financial institutions etc. may prove to be very useful. This would require a reasonable amount of resources for outreach, training or other cooperative activities, but may result in enhanced information exchange.

170. It may also be beneficial to outreach to those (*e.g.* lawyers, notaries, accountants, auditors) involved in the establishment, incorporation, purchase and audit of companies to make them aware of the use of front companies in proliferation networks.

171. Generally, there are limited educational, licensing, registration or oversight requirements for brokers. Flexibility of business operations enables illicit brokers to avoid restrictions by locating in a jurisdiction with little or no regulation of brokering services.

Preventative measures

172. Effective implementation of existing AML/CFT requirements, in particular CDD, record keeping, transaction monitoring, and due diligence with respect to correspondent banking relationships, are relevant measures for a financial institution to mitigate proliferation financing risk.

173. Given that the sources of funding for WMD proliferation can be legal or illegal, well-known indicators or “red flags” for money laundering may be relevant in cases where the source of funds is illegal. However, the risk of proliferation financing is more likely to be present in cases where the source of funds is legal but the end-user or type of goods involved is intended to be obscured. The structural differences between money laundering on the one hand and proliferation financing on the other hand should therefore be taken into account when considering the applicability of AML/CTF requirements.

174. Using existing AML/CFT controls against the threat of proliferation financing has the benefit to financial institutions of allowing them to rely on familiar concepts, processes and procedures to protect against a newly understood risk There may be value in:

- Considering adjustments to AML/CFT controls to adequately detect and prevent proliferation financing.
- Financial institutions applying AML/CFT controls in a risk based manner across all product lines, particularly trade finance.

- Effective use of CDD information by global trade services representatives engaged in trade finance activities, which may require additional training of these representatives in AML/CFT measures.
- Using any information contained in trade finance documentation to verify the goods that are being traded, the final destination, and the parties involved in the trade.

175. Information sharing is critical in enabling a financial institution to address proliferation financing risks. Government may consider providing additional information on threats and risks to allow financial institutions to assess the risks they face from proliferation financing and, where appropriate, to amend CDD and monitoring systems to mitigate the risk.

- Detailed information on entities designated through targeted financial sanctions can be particularly useful to financial institutions.
- Diversion of trade and financial payments through third parties and/or third jurisdictions.
- Jurisdictions with substandard export and financial controls.
- There may be useful public information for financial institutions that is currently made available by export control authorities.
- Information on high risk persons and entities, including front companies.

Investigation

176. Financial information can be useful in proliferation related investigations and prosecutions and relevant authorities should consider its use as a matter of routine in these cases. In particular, financial information is useful for:

- Contributing to uncovering proliferation activities when complemented by information held by competent authorities and other sources.
- Linking entities of concern together, especially given the increasing use of front companies and transhipment points by the proliferation networks in their attempts to evade export controls.
- Demonstrating diversion or infringement of export controls.

177. There are significant amounts of data that are received by financial intelligence units currently in relation to money laundering, terrorist financing and other illicit activity that could contribute to proliferation investigations.

178. There may be some value in reporting suspicions of proliferation financing or other reporting mechanisms.

179. Domestic information sharing mechanisms between government agencies are critical to combating proliferation financing. Given the international dimension of proliferation financing, effective mechanisms to share information between governments is also crucial.

7. BIBLIOGRAPHY

Dolan, John and Walter Baker (2007), *Users' Handbook for Documentary Credits under UCP 600*, No. 694, International Chamber of Commerce, Paris.

FATF (2002), *Report on Money Laundering Typologies*, FATF, Paris, *www.fatf-gafi.org.*

FATF (2003), *Report on Money Laundering Typologies*, FATF, Paris, *www.fatf-gafi.org*.

FATF (2006), *The Misuse of Corporate Vehicles, including trusts and company service providers*, FATF, Paris, *www.fatf-gafi.org*.

FATF (2007), *Guidance on the Risk –Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris, *www.fatf-gafi.org.*

Frantz, Douglas and Catherine Collins (2007), *The Nuclear Jihadist: the True Story of the Man Who Sold the World's Most Dangerous Secrets... and How We Could Have Stopped Him*, Twelve (Hachette Book Group USA), New York.

Gruselle, Bruno (2007), *Proliferation Networks and Financing*, Fondation pour la Recherche Stratégique, Paris, *www.frstrategie.org/barreFRS/publications/rd/RD_20070303_eng.pdf*.

Hinkelman, Edward G. (2002a), *A Short Course in International Payments: How to Use Letters of Credit*, D/P and D/a Terms, Prepayment, Credit, and Cyberpayments in International Transactions, 2nd edition, World Trade Press, Petaluma, California.

Hinkelman, Edward G. (2002b), *A Short Course in International Trade Documentation: The Essential Guide to Documents Used in International Trade*, World Trade Press, Petaluma, California and *www.worldtraderef.com.*

Hinkelman, Edward G. (2004), *Dictionary of International Trade*, 6th edition, World Trade Press, Petaluma, California.

Hinkelman, Edward G., K. Shippey and S. Putzi (2002), *Dictionary of International Trade: Handbook of the Global Trade Community*, 5th edition, World Trade Press, Petaluma, California.

ifs School of Finance and the International Financial Services Association (2007), *The Guide to Documentary Credits*, 3rd edition, text for the certified documentary credit specialist certification, ifs School of Finance and IFSA, Canterbury, Kent and Parsippany, New Jersey.

International Chamber of Commerce (ICC) publications, principally:

ICC (2006), *ICC Uniform Customs and Practice for Documentary Credits* (UCP 600), No. 600, ICC, Paris.

Other ICC publications relevant to this report include:

International Uniform Rules for Demand Guarantees (URDG 458), No. 458, ICC, Paris, 1992.

Supplement to UCP 600 for Electronic Presentation (eUCP), No. 500-3, ICC, Paris, 2002.

ICC Uniform Rules for Collection (URC 522), No. 522, ICC, Paris, 1995.

Incoterms 2000: ICC Official Rules for the Interpretation of Trade Terms, No. 560, ICC, Paris, 2000.

ICC Uniform Rules for Bank-to-Bank Reimbursements Under Documentary Credits (URR 525), No. 575, ICC, Paris, 1997.

International Standby Practices (ISP 98), No. 590, ICC, Paris, 1998.

International Standard Banking Practice for the Examination of Documents under Documentary Credits (2007 Revision for UCP 600), No. 681, ICC, Paris, 2007.

Jones, Scott (2005), *Black Market, Loopholes and Trade Controls: The Mechanics of Proliferation*, presentation delivered at the 2005 Carnegie International Non-Proliferation Conference, Washington DC, 8 November.

Palmer, Howard (1999), *Trade Finance Risk: Documentary Fraud & Money Laundering*, Amer Educational Systems.

United Nations (2006), *Report of the Committee established pursuant to resolution 1540 (2004)*, UN Security Council Committee established pursuant to resolution 1540 (2004), United Nations, New York, *www.un.org/sc/1540/committeereports.shtml*.

ANNEX 1: ELEMENTS THAT MAY INDICATE PROLIFERATION FINANCING

The investigative indicators below serve as a starting point to assist financial institutions in understanding the risk that customers, transactions or other account activity may be associated with WMD proliferation. They are not provided as definitive indicators that WMD proliferation is occurring, as a basis for automated screening, further work would be needed to develop such indicators.

Identifying characteristics that are useful to financial institutions as indicators for possible proliferation financing-related activity poses several challenges, for example:

- Given that the sources of funding for WMD proliferation can be legal or illegal, well-known indicators or "red flags" for money laundering may be relevant in cases where the source of funds is illegal. However, the risk of proliferation financing is more likely to be present in cases where the source of funds is legal but the end-user or type of goods involved is intended to be obscured. The structural differences between money laundering and proliferation financing should therefore be taken into account when considering how indicators could be used.
- Specific information on the risk posed by the end-user or counter-party involved, or technical expertise to evaluate the possible WMD use of goods involved, will generally be needed to fully understand the risk of proliferation financing for a transaction or a customer.[34]
- Proliferators use a range of sophisticated schemes to obfuscate their activities. For example the case studies show that proliferators have used layered letters of credit, front companies, intermediaries, brokers etc. However, existing case studies do not enable us to identify any single financial pattern uniquely associated with proliferation financing, though indicators, if available, may help to identify some of the methodologies used by proliferators.

Nonetheless, the typologies working group has endeavoured, as part of its study of this issue to identify, or adapt, possible indicators of proliferation financing.

It should be stressed that in trade individual financial institutions rarely deal with all counterparties involved, and may not be aware of the activities highlighted below. Some of the indicators also presuppose access to information, *e.g.* on customers of concern, which may not be routinely available to financial institutions, or which financial institutions lack the capacity to use. The list includes both indicators which could provoke initial suspicion of a transaction or customer, and also indicators which would be useful to remove "false positives" through further investigation, but which are not themselves a basis for suspicion. Finally, specific indicators might only be useful at particular stages of the transaction process *i.e.* during initial CDD, during transaction processing ("real time screening"), and after the transaction monitoring post transaction review in investigation of already-suspect activity. The opportunities and capacity to use indicators will therefore vary according to when they can be practically used.

---

[34] Where particular individuals, organisations or countries are the subject of WMD proliferation-finance sanctions programmes or export controls, the obligations on institutions to comply with those sanctions and export controls are determined by countries and are not a function of identifying potential risk. Violations of such sanctions may result in a criminal offence or sanctions in some jurisdictions if funds or financial services are made available to a target, directly or indirectly.

Indicators of possible proliferation financing

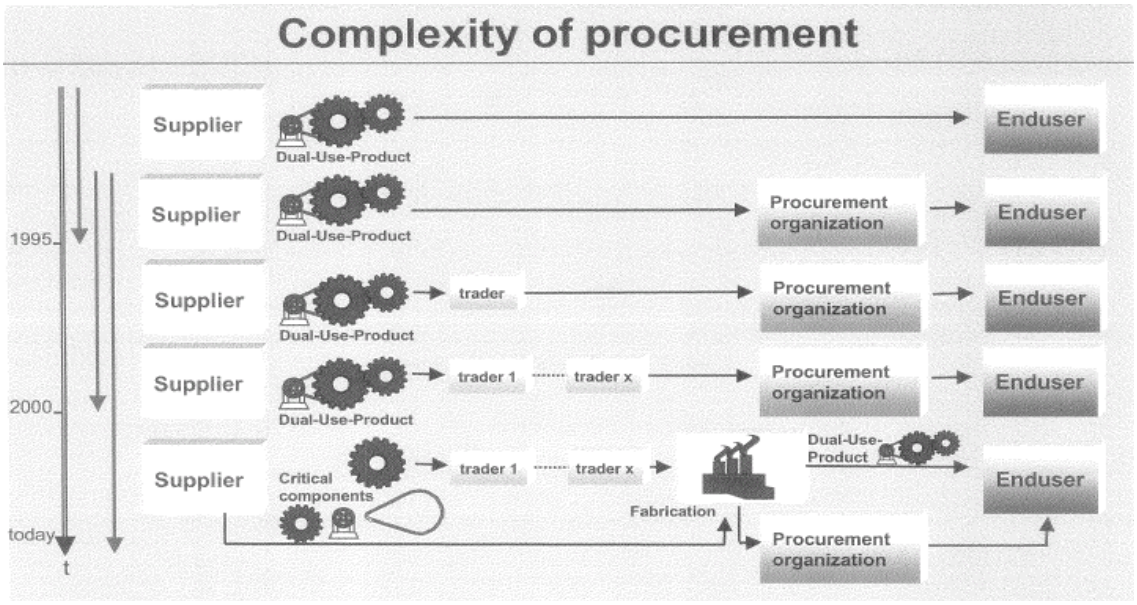
- Transaction involves individual or entity in foreign country of proliferation concern.
- Transaction involves individual or entity in foreign country of diversion concern.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Transaction involves individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (*e.g.* does the country involved normally export/import good involved?).
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (*e.g.* semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Customer activity does not match business profile, or end-user information does not match end-user's business profile.[35]
- Order for goods is placed by firms or individuals from foreign countries other than the country of the stated end-user.[36]
- Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
- New customer requests letter of credit transaction awaiting approval of new account.
- The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Transaction demonstrates links between representatives of companies exchanging goods *i.e.* same owners or management.
- Transaction involves possible shell companies (*e.g.* companies do not have a high level of capitalisation or displays other shell company indicators).
- A freight forwarding firm is listed as the product's final destination.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

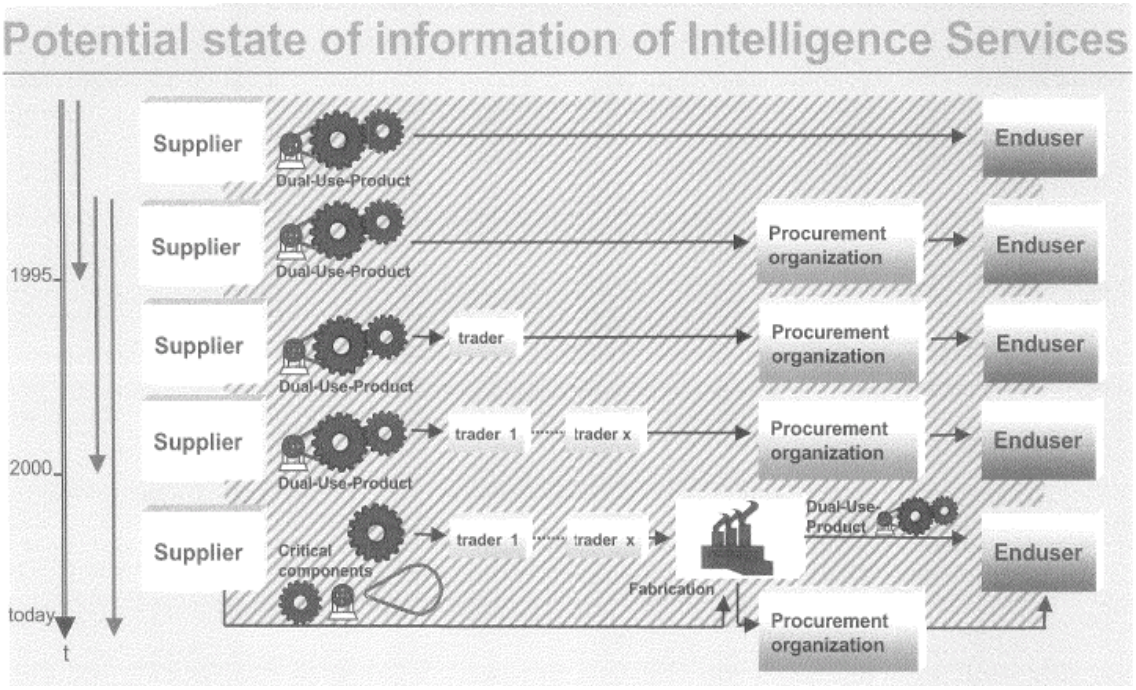
---

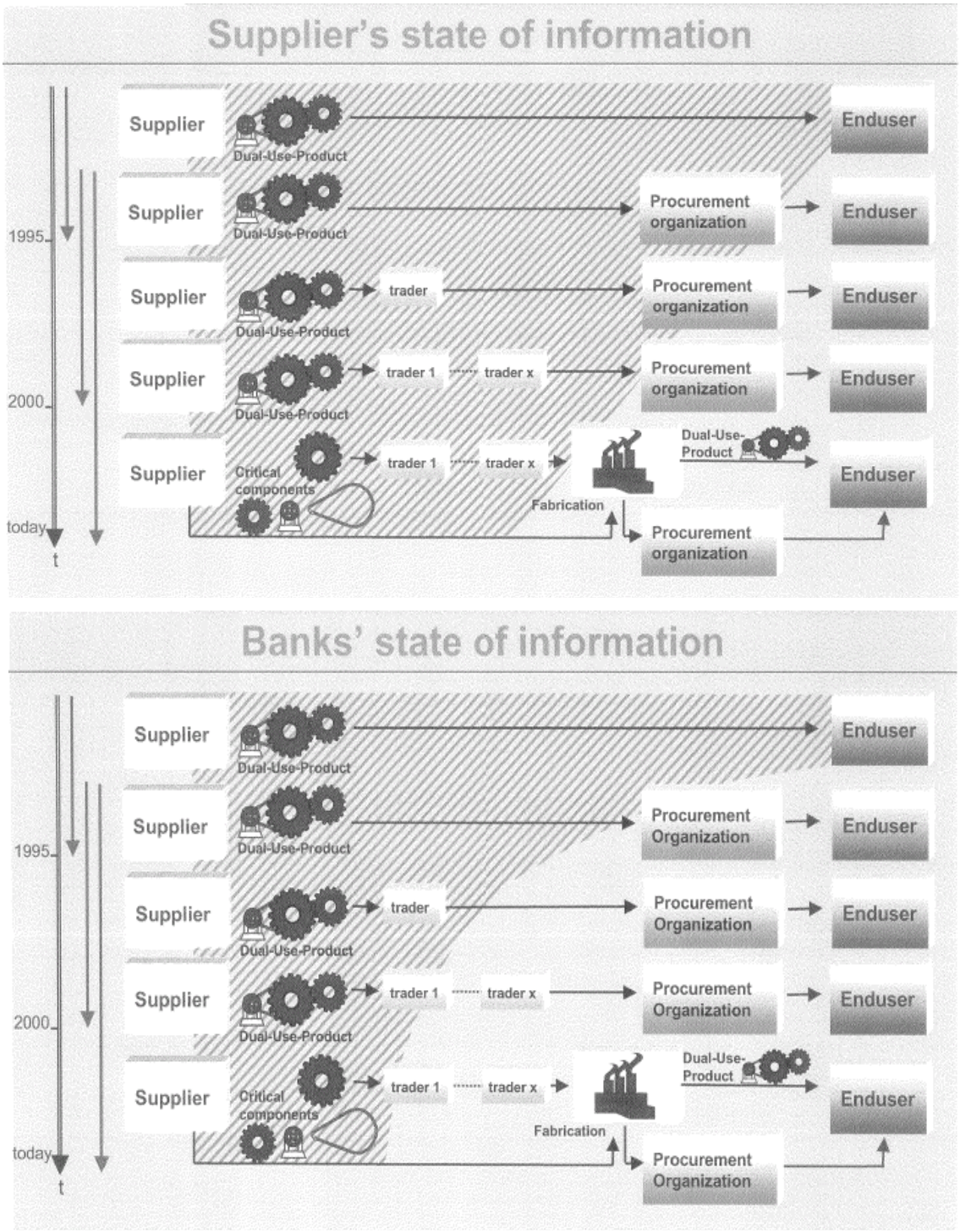
[35] This indicator may also be apparent through credit-risk or other know-your-customer assessments, particularly if a customer is moving into a new line of business. At the transactional level, a transaction involving a product whose capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery, should raise concerns.

[36] In many cases, end-users may not be identified in documentation supporting a transaction. Additionally, wholesale companies routinely have this type of activity as a business model. In cases involving wholesalers, geographic or other factors should be considered in identifying risk.

ANNEX 2: THE COMPLEXITY OF PROCUREMENT NETWORKS OVER TIME







Source: Germany.

ANNEX 3: ADDITIONAL CASES OF PROLIFERATION

While the following cases do not provide any proven direct link of proliferation to the financial sector, they do provide some additional context as to the complexity of the detection of proliferation activity in general. For example, case 16 discusses how financial information may have been useful in investigating illicit activities that were disguised by proliferators through the use of cover names, front companies, false end-users and diversion etc.

Case 19: Customs authorities.

A suspected procurement network operating in Canada attempts to supply targeted entities in **Jurisdiction 1** with goods controlled under Canadian export laws. **Jurisdiction 1** is a jurisdiction of proliferation concern. A shipment of "industrial equipment" was presented for export at a major Canadian port by an exporter that was subject to a Canadian Border Services Agency (CBSA) national security/export control lookout due to suspected proliferation activity. Shipping documents were presented to CBSA indicating that the consignee of the equipment was an import/export trading company. Customs officials formally detain the shipment at the Canadian port for examination and export permit verification. The following documents are analysed:

- Export Declaration Form detailing the exporter, the consignee, the commodity, transportation details (routing, carrier) and the value. The exporter had listed the consignee as an Import/Export Trading Company located in **Jurisdiction 2**, a known transhipment hub. The goods are described as "industrial equipment" without further elaboration.
- Bill of Lading provides cargo shipping information.
- Invoice indicates the value of the "industrial equipment" is $500,000.
- Certificate of Origin indicates the goods originate from **Jurisdiction 3**.
- Export Permit is not presented for the goods (*Note*: Depending on the commodity, its origin and its destination, exporters may be required to indicate a General Export Permit number on their export declaration or they may be required to obtain an Individual Export Permit from competent authorities.

The exporter was the subject of a customs authority lookout (targeted shipment) for procurement activity and has a history of export control contraventions. The consignee was a trading company in a known transhipment country.

The description of the goods as "industrial equipment" was not specific enough to ascertain what the goods actually are or what their intended use might be. The value of the goods is high, which may indicate specialized use or high technological content.

Customs officials at the Canadian port are instructed to contact the exporter and obtain technical specifications for the goods and an end-use certificate from the consignee. The technical specifications reveal that the goods are a "five-axis milling machine", which, depending on their cutting capabilities, are controlled nuclear dual-use goods and subject to Canadian export control laws. The end-use certificate states that the goods are to be used in **Jurisdiction 2** at a wood working plant. Furthermore, a trading company is probably not the true end-user since it is likely the goods will be sold or re-exported. Open source searches indicate that the trading company in **Jurisdiction 2** is state-owned by **Jurisdiction 1**. At this stage, customs authorities have concerns that the milling machine is a controlled commodity and that it will be diverted or transhipped to the nuclear industry in **Jurisdiction 1**.

Canadian Customs officials ask export permit authorities what required export permits are required. Goods originating from **Jurisdiction 3** require a general export permit when destined to **Jurisdiction 2**. Since the exporter did not declare that the goods were being re-exported through Canada, customs authorities issue an administrative monetary penalty to the exporter for failing to properly declare this. There was not sufficient evidence to prove that the goods were destined for jurisdiction 2 and therefore the goods were not seized and were released for export despite suspicions on the part of customs officials.

Case 19 *(Cont'd)*

Numerous indicators maintain the concerns of customs authorities as to the true end-use and destination of the goods. Authorities continue to develop an intelligence file on the exporter and consignee. The intelligence file work-up includes reviewing various intelligence, enforcement, and commercial databases (including both open and classified sources). A review of the Canadian exporting company's previous exports revealed that it had already exported 8 five-axis milling machines with a combined value exceeding $4 million. As such, in addition to the current shipment, CBSA would now expand the intelligence probe to better understand the circumstances (*i.e.* end-users, routing, destination, etc.) surrounding all the shipments of five-axis milling machines (possible controlled nuclear dual-use goods).

Customs officials intercepted the Canadian exporter two weeks later at an airport returning from a trip to **Jurisdiction 2**. A secondary examination of his luggage is conducted under the authority of the customs laws and a bill of lading is discovered in his carry-on baggage, which describes the movement of a milling machine from **Jurisdiction 2** to an electronics company in **Jurisdiction 1**. Classified intelligence indicates that the electronics company is a known front company for **Jurisdiction 1**'s nuclear and missile industries.

In this example, CBSA was unable to seize the five axis milling machine, without proof of the true end-use and ultimate consignee in **Jurisdiction 1**. Proof for transhipment to **Jurisdiction 1** might include:

- Letters of credit from Jurisdiction 1's nuclear industry to the Canadian exporter;
- Financial transactions between the Canadian exporter, the trading company in Jurisdiction 2, the front company in Jurisdiction 1, and Jurisdiction 1's nuclear industry.
- Financial intelligence analysing complete financial proliferation networks linking all the various entities involved.

Source: Canada.

Case 20: Accelerometers

The United States Immigration and Customs Enforcement, Office of Investigations, in conjunction with the Defense Criminal Investigative Service (DCIS), conducted an investigation in which led to a federal indictment against a foreign national. The indictment was for conspiracy to commit offenses against the United States in connection to exporting Endevco 7270A-200K accelerometers, which are designated as a defense article on the United States Munitions List and cannot be exported from the United States without permission from the United States Department of State. The Endevco 7270A-200K accelerometer has many military applications including use in "smart" bombs, missile development and the measurement of nuclear and chemical explosives.

From April 2007 through October 2007, ICE agents conducted undercover operations, in which an identified foreign national conspired with agents to export the Endevco 7270A-200K accelerometers in violation of United States Export laws. Undercover agents were advised that if the items were delivered overseas in proper working order, larger orders would follow. Undercover agents along with identified suspects negotiated price, payment, and delivery terms of the accelerometers in furtherance of the conspiracy. Undercover discussions included the delivery of the accelerometers to either a third party country or the country of final destination. Financial terms were discussed between the Undercover agents and the violator utilising the formal financial sector through either an escrow account for payment or making payments through bank wire transfers.

The defendant has been charged under Title 18, of the United States Codes, Section 371, with conspiracy to Commit offenses Against the United States and faces a maximum penalty of five (5) years in prison and a $250,000.00 fine.

Source: United States.

Case 21: Shipping of electronics to a number of countries

Canadian **Individual A** is the sole owner of Canadian **Company A**, whose business includes the shipping of electronics to a number of countries. Canadian **Individual A** contacted Canadian **Company B** to purchase a number of computer chips (power amplifiers) designed for use in radar and satellite communication systems. These goods are dual use with potential military applications and are subject to export controls. **Individual A** reported the end-user as Canadian **Company C** and refused to allow Canadian **Company B** to meet with representatives of Canadian **Company C**. Canadian **Individual A** ultimately cancelled the order entirely.

Significant suspicions were raised on the part of Canadian **Company B** once Canadian **Individual A** refused to coordinate a meeting with Canadian **Company C**. The addresses given by Canadian **Individual A** on the US Traffic in Arms Regulations (ITAR) form for both the purchaser (Canadian **Company A**) and the purported end-user (Canadian **Company C**) were the same.

Further investigation revealed that Canadian **Company C** is actually based overseas, and is also run by Canadian **Individual A** and another person. Had the purchase of computer chips from Canadian **Company B** gone through, the items would have been shipped through Canada overseas.

The following year, an intermediary for the military of a foreign country requested a purchase of US-origin military-grade night-vision cameras from the same Canadian **Individual A**. The cameras have potential dual-use WMD applications in addition to regular military use and are subject to export-controls. Canadian **Company A** placed an order for one camera with US **Company 1**. US **Company 1** notified US authorities, who confirmed that the camera, after arriving in Canada, was then re-exported overseas and is currently located near an important nuclear site in a country of proliferation concern.

In addition, Canadian **Individual A** has been involved in other procurement deals designed to circumvent US export restrictions using Canadian **Company A**. For instance, Canadian **Company A** is now believed to be in the midst of procuring F-5 fighter aircraft spare parts from US **Company 2**, also on behalf of Foreign **Company X**, purportedly for a foreign Air Force. Canadian **Company A** has also attempted to re-label a US-origin airplane propeller as originating in another country in order to avoid prohibitions regarding shipment and re-export of US-origin goods. Although this particular shipment was stopped by Canadian authorities, other similar orders have been carried out. Canadian **Company B** has also fielded requests for other military-related goods, such as helicopter parts and jet fuel, although it is not known if these particular orders have been completed.

Source: Canada.

Case 22: Use of intermediaries to circumvent export restrictions

Canadian **Company A** deals in medical products and laboratory equipment and was in contact with Foreign **Company X** regarding the sale of multiplexers and potentiograph laboratory equipment. Foreign **Company X** is a procurement entity associated with a foreign nuclear programme of proliferation concern. Inquiries revealed that Canadian **Company A** has ongoing business dealings providing potential dual-use goods to a number of foreign enterprises, including Foreign **Company Y**. Foreign **Company X** is known to utilize Foreign **Company Y** as an intermediary, as part of its deceptive practices to avoid revealing the foreign nuclear programme as the end-user of purchased equipment. Goods are instead described as being for "educational purposes".

Further investigation revealed that the proprietor of Canadian **Company A**, Canadian **Individual A** regularly engaged in deceptive practices to conceal the end-user of dual-use equipment. Some deceptive techniques used in this particular case include the following:

- **Individual A** frequently provided the name of a Canadian University as the end-user for US-origin and other goods, despite having no actual connection with the university. The products would then be re-shipped to various foreign countries via commercial courier, with the description "laboratory equipment" or "medical instruments" given on the customs declaration, regardless of the true nature of the product being exported.
- Canadian **Company A** falsified documents in order to hide US-origin goods, re-labelling them as Canadian products manufactured in a south-east Asian country in order to permit export to embargoed countries.
- Canadian **Company A** exploits the fact that a country's export authorities generally do not inspect exported items as rigorously as imported items.
- Canadian **Company A** exploits a loophole in export reporting requirements for goods valued at less than $2,000.00 dollars, by re-invoicing products at a far lower value to avoid having to complete a paper export declaration.
- Canadian **Company A** is also involved as part-owner of Foreign **Company Z**, which it uses as the principal point of transit for goods going from Canada to overseas.

In addition to a number of potential nuclear/WMD dual-use exports to the companies noted above, Canadian **Company A** also conducts business with several other entities of procurement concern. These entities have been connected to procurement activities on behalf of various nuclear/WMD programmes in different countries of proliferation concern. Canadian **Company A** is currently the subject of a joint investigative effort by Canadian agencies aimed at uncovering the nature and extent of its procurement activities on behalf of the nuclear/WMD programmes of several high-interest countries.

Source: Canada.

Case 23: Illicit Brokering

A suspected procurement network operating in Canada aimed to supply entities in a jurisdiction of proliferation concern with controlled and strategic goods.

While executing a search warrant related to an offence of the *Customs Act* and the *Export and Import Permits Act* at the business address of the Canadian exporter, Customs authorities uncover shipping documents and commercial invoices related to a shipment of titanium-stabilized stainless steel tubes with an outer diameter of 750mm and a wall thickness of 2.5mm (controlled under 6-6.C.9 of the ECL). This shipment was not related to the offence being investigated. The documents related to this shipment indicate the tubes were manufactured in a European country; purchased by the Canadian company; moved by rail to a second European country; loaded into a maritime shipping container; shipped to a Free Trade Zone and once there, re-manifested and shipped to the jurisdiction of proliferation concern.

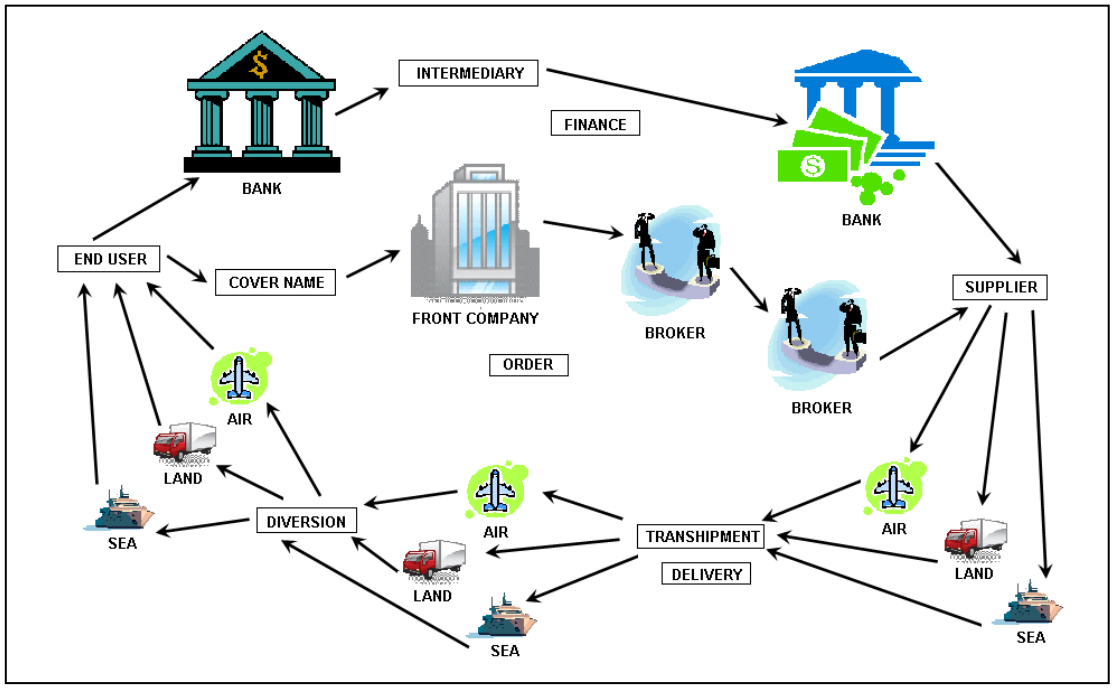
CBSA did not have enough evidence to enable it to act upon this illicit brokering activity. Furthermore, the above example is based on the fact that CBSA authorities had obtained a search warrant on an unrelated matter. If CBSA had not been searching the business records, this infraction would have gone undetected. However, financial information could have formed the basis for an initial investigation.

Source: Canada.

Case 24: Traditional counter proliferation making use of financial information

This diagram represents the procurement process and the start point for an analysis of proliferation networks. Counter proliferation has traditionally focussed on the bottom two aspects of the process.

This model can be used to describe purchases made on the open market and transfers between proliferators.



When purchases are made on the open market only a few entities within the diagram will be aware of what they are doing. In some cases only one entity will know. It is unlikely entities within the delivery or finance part will have sight of what is occurring. For example, it may be that only the end-users and the representative of the front company that are aware of the true destination and end-use for the goods.

When the transfer is between proliferators more of the entities involved will be aware that they are engaged in illicit activity. However these transactions still utilize commercial practises and routes some entities involved in the procurement and transportation may be unaware of that occurring. For example while the entities representing the supplier and end-user – the middle part of the chain would be aware the transfer is associated with a WMD or BM programme. They may choose to transport the goods by commercial carrier who would be unaware of the nature of the transfer.

Source: United Kingdom.

Case 25: Kahn

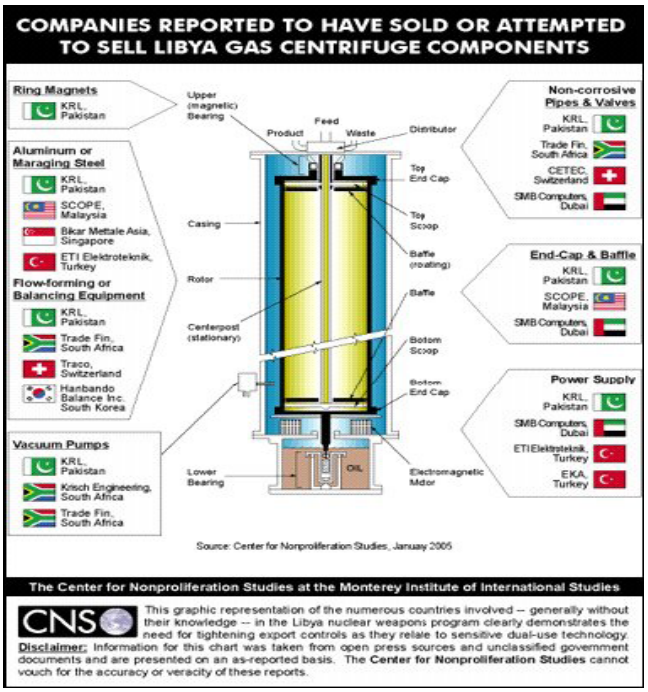
The Khan-case (which consists of several different proliferation cases over a long period) concerned nuclear weapon programs in several jurisdictions of proliferation concern. The process of proliferation for each item to be constructed consisted of many steps in order to disguise the activities of the network and the true nature and end-use of the goods. Many individuals, companies and countries were – knowingly or in good faith – involved. There is not much published concerning the financing in the Khan proliferation networks, but at least the following is mentioned in "Proliferation Networks and Financing" by Bruno Gruselle (Fondation pour la Recherche Stratégique, March 2007):

"Although some operations appear to have been settled in cash, others were settled through international transfers within the framework of duly established contracts. For example, this is the case for the contract made between the *Gulf Technical Industries* (GTI) company and SCOPE, for an amount of 13 million dollars."

"In terms of the financial organization, the few data available highlight two types of transaction:

- Inter bank: for remuneration of agents or suppliers outside the network. In other words, transfers between suppliers, intermediaries and/or front companies. Thus, the contract between SMB and SCOPE appears to have been financed conventionally, probably through letters of credit or bills of exchange.
- Cash transactions within the network and with customers. The amounts thus obtained (possibly in several payments) could then have been deposited in bank accounts of emerging or offshore countries before transactions were made between banks for final beneficiaries. Even if payments were made in cash, some operations could have been made through written contracts between Khan (and/or Tahir) and the intermediary concerned."

An illustration from the Centre for Non-proliferation Studies concerning gas centrifuge components to Libya illustrates the puzzle of proliferation of WMD – and also illustrates why detection is so difficult:



Many centrifuges are needed and a numerous components are required for each centrifuge. Several entities will be involved in the different networks used to acquire the components – including in payments and financing – but if someone sells e.g. 10 vacuum pumps to a country which is not a country of special concern one may not have WMD as the first thought.

Source: Gruselle, Bruno, (2007).

ANNEX 4: RELEVANT CONVENTIONS AND INITIATIVES

1. Nuclear Non-Proliferation

1.1 INTERNATIONAL TREATIES

Treaty on the Non-Proliferation of Nuclear Weapons (NPT)

The NPT aims at preventing the spread of nuclear weapons outside the five States which are recognised by the NPT as nuclear weapon States (NWS): France, the People's Republic of China, Russia, the United Kingdom, and the United States. These NWS have agreed not to transfer nuclear weapons or other nuclear explosive devices and not in any way to assist, encourage, or induce a non-nuclear weapon state (NNWS) to acquire nuclear weapons.

NNWS which are party to the NPT agree not to receive, manufacture or acquire nuclear weapons or to seek or receive any assistance in the manufacture of nuclear weapons. They also agree to accept safeguards by the International Atomic Energy Agency (IAEA) to verify that they are not diverting nuclear technology from peaceful uses to nuclear weapons. In return, NNWS are granted the inalienable right to use nuclear energy for peaceful purposes.

190 States are party to the NPT.

1.2 INTERNATIONAL ORGANISATIONS

The International Atomic Energy Agency (IAEA)

The IAEA is an independent intergovernmental organisation under the aegis of the United Nations and is the world´s centre of cooperation in the nuclear field. The Agency works with its Member States and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies. Three main pillars – or areas of work – underpin the IAEA´s mission: Safety and Security; Science and Technology; and Safeguards and Verification. The IAEA reports annually to the UN General Assembly and, when appropriate, to the UN Security Council. It also works closely with the World Customs Organisation on security and trade issues, the Universal Postal Union on mail security issues, and Interpol and Europol in combating illicit nuclear trafficking.

The IAEA conducts inspections in countries that have safeguards agreements with a view to verifying that those countries are using nuclear material peacefully and providing recommendations on ways to improve the accountability and control of nuclear material. It also provides training at the international, regional and national levels concerning the security of nuclear and radioactive materials. In addition, the IAEA helps countries to obtain the necessary equipment for physically protecting nuclear and radioactive materials, including equipment that assists in the detection of cross-border smuggling of such materials.

In 1997, a model Additional Protocol to the NPT was produced by the IAEA. The adoption of the Additional Protocol is a voluntary measure for non-nuclear weapons states parties, designed to strengthen and expand existing IAEA safeguards for verifying that they only use nuclear materials and facilities for peaceful purposes.

1.3 EXPORT CONTROL REGIMES

The Nuclear Suppliers Group (NSG)

The NSG is one of four informal and voluntary export control regimes. It consists of a group of nuclear supplier countries which create Guidelines for exports of nuclear goods and nuclear related dual-use goods. The NSG Guidelines aim to ensure that nuclear trade for peaceful purposes does not contribute to the proliferation of nuclear weapons or other nuclear explosive devices, and to mitigate the risk of acts of nuclear terrorism. Participants seek to coordinate national export licensing efforts to prevent nuclear proliferation.

The NSG has 45 participants. The European Commission participates as an observer.

The Zangger Committee

The Zangger Committee, also known as the "NPT Exporters Committee", contributes to the interpretation of article III, paragraph 2, of the Nuclear Non-Proliferation Treaty (NPT) and thereby offers guidance to all parties to the Treaty. The main significance of this paragraph is that parties to the Treaty should not export, directly or indirectly, nuclear material and equipment to non-nuclear-weapon States unless the export is subject to International Atomic Energy Agency (IAEA) safeguards. By helping to establish and update control lists of nuclear equipment, the Zangger Committee helps to prevent the diversion of exported nuclear items from peaceful purposes to nuclear weapons or other nuclear explosive devices.

2. Missiles

2.1 EXPORT CONTROL REGIMES

The Missile Technology Control Regime (MTCR)

The MTCR is one of four informal and voluntary export control regimes. It aims to ensure the non-proliferation of ballistic missiles, cruise missiles and other unmanned delivery systems capable of delivering weapons of mass destruction. Partners of the MTCR seek to coordinate national export licensing efforts aimed at preventing the proliferation of these means of delivery by defining Guidelines for the export of relevant systems and related dual-use goods.
The MTCR has 44 partners.

3. Chemical Weapons

3.1 INTERNATIONAL TREATIES

The Chemical Weapons Convention (CWC)

The CWC prohibits all development, production, acquisition, stockpiling, transfer, and use of chemical weapons. It requires each State Party to destroy chemical weapons and chemical weapons production facilities it possesses, as well as any chemical weapons it may have abandoned on the territory of another State Party. The CWC does not prohibit production, processing, consumption, or trade of related chemicals for peaceful purposes, but it does establish a verification regime to ensure such activities are consistent with the object and purpose of the treaty.

The verification provisions of the CWC not only affect the military sector but also the civilian chemical industry, world-wide, through certain restrictions and obligations regarding the production,

processing and consumption of chemicals that are considered relevant to the objectives of the Convention. The most important part of the verification regime, however, are regular inspections which are conducted by the Organisation for the Prohibition of Chemical Weapons (OPCW). The CWC maintains only controls on chemicals, but does not control production technology.

183 States are party to the CWC.

3.2 International Organisations

The Organisation for the Prohibition of Chemical Weapons (OPCW)

The Organisation for the Prohibition of Chemical Weapons (OPCW) is responsible for the implementation of the Convention. The OPCW is mandated to ensure the implementation of its provisions, including those for international verification of compliance with the Chemical Weapons Convention. It also performs monitoring and conducts inspections to verify that declared chemical weapons production facilities have been deactivated and declared weapons stockpiles destroyed. Inspectors also verify the consistency of industrial chemical declarations and monitor the non-diversion of chemicals for activities prohibited under the Chemical Weapons Convention.
To address the threat of chemical terrorism (*i.e.* the use of chemical weapons by terrorists to threaten, injure, or kill people), the OPCW works towards chemical disarmament and to ensure that chemicals which are produced for peaceful purposes are not misused.

3.3 Export Control Regimes

The Australia Group

The AG is one of four informal and voluntary export control regimes which controls chemical and biological substances, as well as production equipment. The Group meets annually to discuss ways of increasing the effectiveness of participating countries' national export licensing measures to prevent would-be proliferators from obtaining materials for CBW programmes.

The AG has 41 participants including the European Commission.

4. Biological Weapons

4.1 International Treaties

The Biological and Toxin Weapons Convention (BTWC)

The Convention bans the development, production, stockpiling, acquisition and retention of microbial or other biological agents or toxins, in types and in quantities that have no justification for prophylactic, protective or other peaceful purposes. It also bans weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.

156 States are party to the BWC.

4.2 Export Control Regimes

The Australia Group (see section 3.3)

5. Conventional Weapons

5.1 EXPORT CONTROL REGIMES

The Wassenaar Arrangement (WA)

The WA is one of four voluntary and informal control regimes and concentrates on export controls for conventional arms as well as related dual-use goods and technologies. The WA contributes to regional and international security and stability and aims at preventing destabilising accumulations of conventional arms. The WA follows agreed Guidelines and Procedures, including the Initial Elements, the founding document of the WA. The 40 WA participating States implement export controls on the basis of WA control lists, agreed guidelines and best practices via national legislation and report transfers and/or denials of specified controlled items (arms and dual-use gods).

The WA has 40 participating States.

6. Other non-binding Measures

The Proliferation Security Initiative (PSI)

The Proliferation Security Initiative (PSI) is an informal network of cooperating nations that are committed to stopping the trafficking of weapons of mass destruction, their delivery systems, and related items to and from states and non-state actors of proliferation concern. The PSI was created in 2003 as an innovative complement to more formal non-proliferation regimes. More than 85 countries have endorsed the PSI Statement of Interdiction Principles (4 September 2003). PSI participating states develop a broad range of legal, diplomatic, economic, law enforcement, and other tools to assist in interdicting shipments of proliferation concern consistent with national legal authorities and relevant international law and frameworks. To date, PSI partner states have conducted over 30 interdiction training exercises involving more than 70 nations. These exercises increase the interoperability of PSI participants, improve interdiction decision-making processes, and enhance the interdiction capacities of participating states.

ANNEX 5: ELEMENTS OF EXPORT CONTROL SYSTEMS

Export control systems can vary from jurisdiction to jurisdiction, including each jurisdictions lists and due diligence for controlled goods. At a minimum, jurisdictions that implement export controls tend to licence the exports of certain goods, as identified by the four export control regimes. A truly comprehensive regime may require catch-all clauses. Many jurisdictions may consider the following elements in their export control systems:

Preventive export control

- International information sharing.
- National open source information (websites, conferences, seminars, etc.).
- Outreach activities to the private sector:
    - Legal basis
    - International sanctions and UN-resolutions
    - Procurement methodology
    - Countries/entities/organisations/persons of concern
    - Red flags
    - End-user/purchaser check

Export control

- Export authorisation.
- Special authorisation for certain products, *e.g.* weapons, chemicals or CBRN-material.
- Customs control – screening:
    - Licenses
    - Certificates
    - Shipping documents
    - Other documents
- Technical assessment of exported items
- Customs control – border:
    - Spot checks
    - Front companies
    - Diversion
    - Trans-shipment and transit cargo

Investigative export control authorities

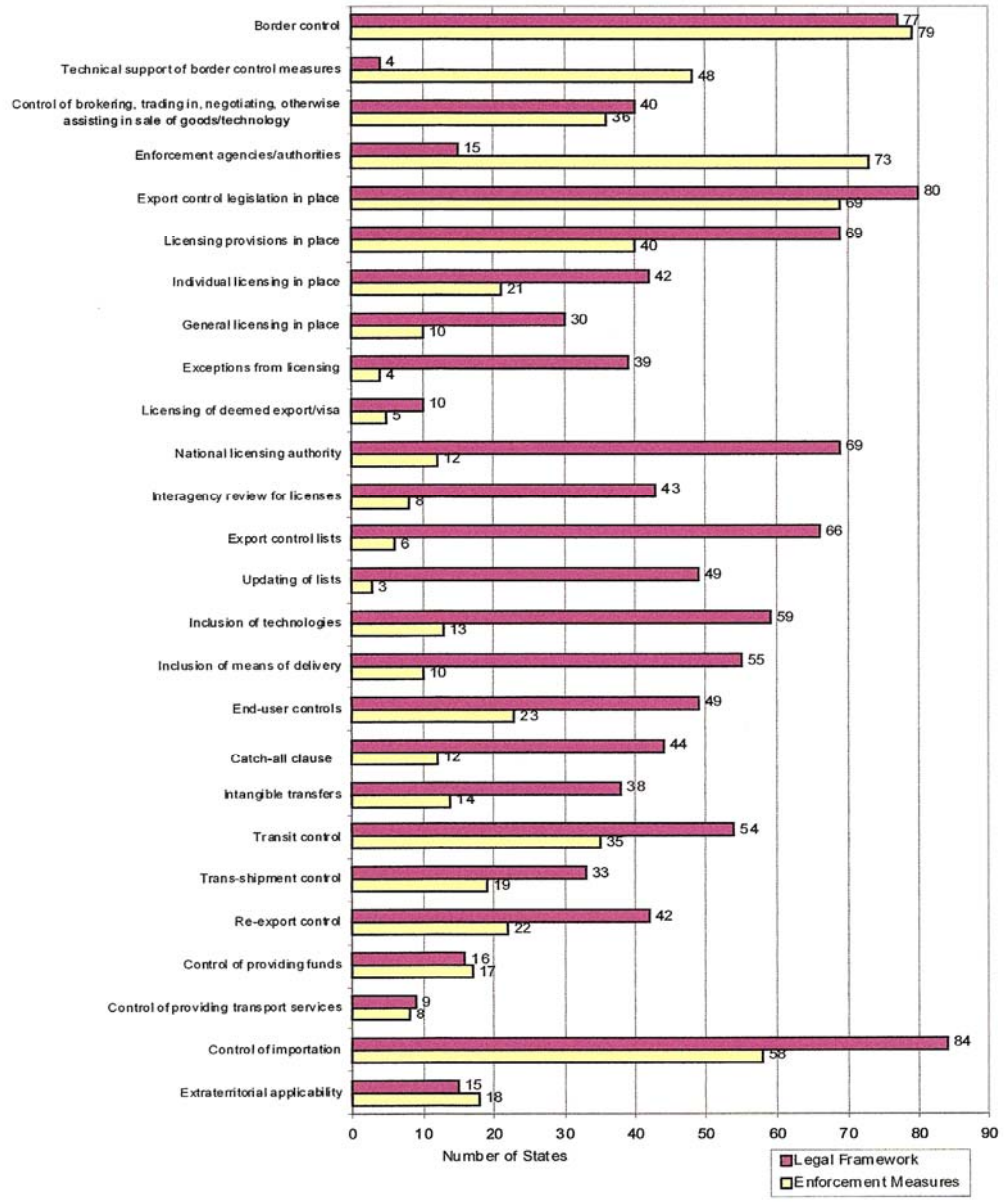
- Licensing authorities:
    - Applications
    - Denials
- Customs:
    - Authorisations
    - Surveillance
- Intelligence
- Security
- Police authorities
- Other public authorities

ANNEX 6: EFFECTIVE BORDER AND EXPORT ENFORCEMENT

Annex IX

States reporting on national legal framework and enforcement measures under paragraph 3 (c) and (d)

Border and export controls



ANNEX 7: INFORMATION IN DOCUMENTS WHICH MIGHT BE CALLED FOR AND PRESENTED UNDER A LETTER OF CREDIT PRESENTED AS PART OF A DOCUMENTARY COLLECTION

Note. Similar documents to those described below may be presented as part of documentary collection order, but unlike the L/C scenario *i)* without any reference to a letter of credit *ii)* the draft should not be drawn on the bank and *iii)* the bank will not be examining the documents for the same detailed consistencies.

The *Draft* or Bill of Exchange (not always required) provides formal evidence of debt under a letter of credit and is presented with all other documents unless stipulated otherwise. A Draft may contain information on:

- Value of Draft, date of payment and payment terms *e.g.* "at sight", "30 days after sight", "60 days after Bill of Lading Date".
- Date Exporter presents documents to the "available with" Bank (not normally required).
- Letter of credit reference number assigned by the Issuing Bank (if required by credit).
- Date the letter of credit was issued (not normally found on a draft).
- Name and address of the Issuing Bank (if the drafts are drawn on the issuing bank).
- Name and address of the bank on which the Drafts are to be drawn.
- Signature of an authorised signing officer of the Company and the Beneficiary's name as shown on the letter of credit.

The *Commercial Invoice* is the accounting document through which the exporter charges the importer for goods and services purchased. The Invoice gives details about:

- Merchandise weight, quantity and price and currency.
- The name and address of Exporter and the Importer.
- The number of copies presented and signed if required.
- The trade term listed, *e.g.* C.I.F., F.O.B etc.

The *Transport Document* (or Bill of Lading, Airway Bill, Railway Consignment Note) is a document issued by the carrier that describes the goods that have been accepted for carriage. In some forms, the Bill of Lading may also act as a document of title to the goods and should include information that is consistent with the letter of credit:

- Information on the merchandise (usually a general description).
- The points of loading and discharge.
- To whom the Bill of Lading is consigned.
- The date of shipment.

The *Insurance Document* is a guarantee in part or in whole (depending on the terms and conditions) by an insurance company, specifying the goods shipped on a named vessel, indicating the applicable coverage, and showing to whom loss is payable.

The *Certificate of Origin* notes the country where the goods were produced. The *Certificate of Inspection* offers an opinion that the specified quality and quantity related conditions have been met. These documents should be dated on or before the Bill of Lading date.

A *Packing List* is usually supplied by the exporting shipper in cases where a diversified shipment is packed in several packages or containers. The list will show the contents of each box or case identified by a specific number. A *Weight Certificate* is supplied by the Exporter, at the request of the Importer. It certifies the weight of each large unit in a shipment or the net and gross weights of packages containing smaller units. It is of particular value when the price of the goods is based on weight and, also, is often used by the carrier in arriving at the weight to be recorded on the Bill of Lading as a basis for the freight charges.

- The quantity of units/weights should match the Commercial Invoice (this may or may not agree based on how the weights are calculated by the various parties involved).
- The breakdown of merchandise/weight per carton, package or container should be shown if requested in the letter of credit.