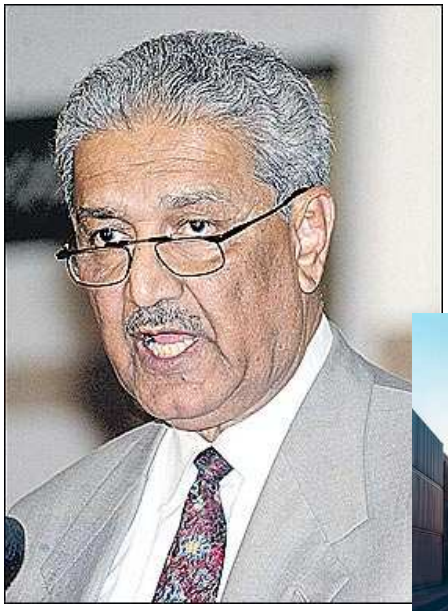
Fondation pour la Recherche Stratégique

Recherches & Documents

Proliferation Networks and Financing

Bruno Gruselle

(March 3rd 2007)



Fondation pour la **R**echerche **S**tratégique • 27, rue Damesme • 75013 PARIS
Tel.: 01 43 13 77 77 • Fax: 01 43 13 77 78 • http ://www.frstrategie.org

Siret 394 095 533 00045 • TVA FR74 394 095 533 • Code APE 732Z
Fondation reconnue d'utilité publique – Décret du 26 février 1993

CONTENTS

Introduction

Several tens of centrifuge components were discovered on their way to Libya when the German ship *BBC China* was intercepted in October 2003, thus revealing the existence of a large-scale network in nuclear technology smuggling. Its founder, Dr Abdul Qader Khan, considered as the father of the Pakistani nuclear bomb, had succeeded in creating a commercial system designed to assist countries aspiring to the possession of nuclear weapons in their quest, in return for payment, making use of contacts woven within the framework of the Pakistani nuclear bomb program.

This enterprise illustrates the development of a *second-tier* proliferation phenomenon by which developing countries mutually assist each other in their efforts to develop and possess nuclear weapons or missiles[1]. Everything suggests that the Khan network extended beyond simple assistance to nuclear programs and contributed to setting up technical cooperation between its customers. For example, this is the case for the development of the Nodong missile and its Pakistani variant (Ghauri) and the Iranian variant (Shahab-3).

Although attention has been focused on the Khan network, there is no doubt that several more or less interconnected systems were set up to bypass the non-proliferation system. Work done by the *Iraqi Survey Group* demonstrated that Saddam Hussein's Iraq had set up a system designed to circumvent the embargo and acquire goods from other countries for use in prohibited programs. Similarly, the underground activities of the North Korean regime probably include the supply of proliferation technologies to customers such as Iran, Pakistan and even Syria. Other proliferation networks such as that which led to the transfer of Kh-65 missiles to Iran and the Popular Republic of China, are more comparable with "conventional" criminal enterprises taking advantage of the weaknesses of export control systems.

Developments and changes to these networks, some of which have existed for several decades, illustrate several serious trends in terms of proliferation.

Firstly, export control tools set up by some States are found to be effective in preventing the acquisition of key technologies for the nuclear and missile domains. But on the other hand, technical progress is tending to make some goods previously reserved for military use commonplace. At the same time, the spectrum of technologies and goods that could potentially be used for proliferation projects is being quickly broadened. Western States are literally facing an explosion in the quantity of goods and services that should be controlled because of their possible application to nuclear programs or missiles; simply looking at recent changes to lists of dual-use goods controlled by supplier regimes demonstrates the magnitude of the task facing national inspection authorities.

Furthermore, the worldwide distribution of some of these technologies (for *a priori* legitimate applications) makes it almost impossible to strictly control their destination. The involvement of the Malaysian SCOPE Company in the Khan network illustrates the difficulty; in a country in which there are few or no strict controls over transfers of sensitive goods, a company can freely produce and export goods without knowing that they are

[1] C. Baum & C. F. Chyba, « Proliferation Rings », *International Security*, Vol. 29, No. 2, Fall 2004, p. 5.

intended for a nuclear program[2]. Thus, the heteroclite nature of national control systems enables proliferation networks to acquire goods that members of supplier regimes refuse, from some other countries.

The increase in world trade in material and immaterial goods tends to facilitate this task.

Proliferators have made massive use of the main hubs of world trade like Dubai and Singapore that handle large volumes of transactions without having developed appropriate control systems, as turntables for equipment flows, particularly by setting up local front companies for the purpose of managing the acquisition of dual-use goods in the West and transferring them to their final destination.

The development of communication means (Internet or inexpensive media capable of storing large quantities of data) has enabled suppliers to transfer know how to their customers almost with impunity, and even to delocalize some of the technical support for programs. Furthermore, in the academic domain, the increase in scientific cooperations and the acceleration of foreign training policies have made a direct contribution to the increase in the technical expertise of executives who might participate in nuclear or missile programs.

Finally, it is quite clear that paradoxically, the proliferation phenomenon has become privatized. Although some States directly involved in the supply of proliferation goods have officially renounced this activity, existing networks continue to operate more or less independently. The question of the degree of complicity of governments and even managing authorities nonetheless arises in the Chinese and Pakistani cases.

These trends have one practical consequence for proliferation countries; although critical know how has become more difficult to obtain because it is better protected by the countries holding it, most of the goods necessary for development of a program are accessible. Proliferation networks benefit from economic internationalization tools that make it easier for them to achieve one of their main objectives, namely to circumvent prohibition systems in order to supply their customer.

[2] Malaysian investigation report on the activities of B.S.A. Tahir and SCOPE, February 20 2004.

TOWARDS A MODEL OF PROLIFERATION NETWORKS

In order to obtain the technologies they need, proliferation players need to be capable of:

- accessing dual-use components through discrete acquisition (direct or indirect);
- obtaining and understanding and controlling critical know-how[3];

This can be done using two different systems:

- Create a national acquisition tool, backed up by an independent or quasi-independent development effort. The Iraqi case made use of this approach: the acquisition network performs logistics, financial and administrative functions but it is not directly involved in the technical effort.
- Call upon an external supplier capable of transferring critical know how, or even of supplying a turnkey capacity, by proposing a series of complementary technical and trade services. In particular, this supplier must be capable of participating in the technical evaluation of the need and production of a proposal, guaranteeing the transfer of the related material and immaterial goods and integrating them for the benefit of the customer. This is the case for the Khan network, or the North Korean missile technology transfer system.

Nevertheless, the boundary between suppliers and buyers is porous. An acquisition network may become a purveyor of technologies. For example, the existence of a "Nodong for centrifuges" transaction between the North Korean network and the Khan network is sometimes mentioned in open-sources papers[4]. Similarly, the Pakistani nuclear network created during the 1970s to support Islamabad's acquisition efforts has become the first "proliferation SuperMarket"[5].

A systemic study of their operation is essential in the effort to find solutions adapted to this new proliferation era. The first objective is to identify the structure of the two major types of networks to determine the principle functions performed and methods used for management of flows (financial, goods, know how). The two best-documented cases, the Khan network and the Iraqi system, can be used to identify key mechanisms that control the structure of acquisition and supplier networks.

The other objective is to model the two major types of proliferation networks. Finally, conclusions have to be drawn about conditions under which networks function and therefore their vulnerabilities.

TO ENABLE THE CHOICE OF SUITABLE SOLUTIONS IN RESPONSE TO CHANGES IN NETWORKS

The security community must find specific solutions in response to systems designed and constructed to make use of weaknesses in treaties and in regimes forming part of the conventional non-proliferation framework.

[3] For empirical knowledge and equally for knowledge acquired through experience. See Alexander H. Montgomery, « Ringing in Proliferation », in *International Security*, Vol. 30, No. 2, Fall 2005, p. 176.
[4] Gaurav Kampani, « Second Tier Proliferation: The Case of Pakistan and North Korea », *Nonproliferation Review*, Vol. 9, No. 3, Fall/Winter 2002.
[5] Free translation of « *nuclear WalMart* ».

American efforts on the subject have been widely publicized; international tools (PSI), bilateral agreements (CSI, *Megaports*) and national initiatives (control of immaterial flows, financial sanctions, monitoring of foreign students), and many criticisms have been made about the form and the content of the US non-proliferation initiatives.

Without reopening a discussion about Washington's supposed unstated intentions, it is worthwhile analyzing the relevance of existing solutions with respect to the observed phenomenon and providing elements of judgment on their exhaustiveness and their limits.

The purpose of the study is to propose practical solutions to extend and reinforce the existing system. In particular, financial, material and immaterial flow management tools deserve special attention since quantities of funds and equipment considered in proliferation phenomena are very large, although the quantities actually passing through terrorist enterprises are apparently small[6].

Furthermore, the economic and political feasibility of some positive incentive measures must also be studied carefully, since they appear to be complementary to more repressive approaches.

[6] The North-Korean ballistic trade is usually believed to provide Pyongyang with between 500 million and one billion dollars annually. The scale of North Korea's missile income is probably a few hundred million dollars per year.

1 – Systemic analysis of supplier and requester networks

There is no single pathway leading to the development of proliferation networks. Each tool set up by players to acquire or supply proliferation goods is specific and satisfies constraints and needs related to the immediate environment (political, security, economic and cultural) of the programs that it supplies[7]. However, the controlling principles that govern the appearance of such networks remain globally identical, even if individual situations of the players concerned are different. Thus, two essential principles should be mentioned in a first analysis:

- The will to hold nuclear weapons and their carrying means.
- The impossibility of obtaining the required goods legitimately and/or legally.

The existence of a strong demand from some States has always been the driving force for proliferation, but the structure of networks designed to satisfy this demand is new. It has been made possible by three concomitant phenomena.

Firstly, the increase in worldwide trade flows and the widespread development of tools for managing them facilitated layering of material and immaterial transfers. Like other trafficking organizations, proliferation networks conceal themselves in dark corners of world trade that has become difficult to monitor strictly[8]. Payments for transfers are made through front companies, technical or financial intermediaries that take advantage of lax controls in some States.

Secondly, the fact that some technologies and goods that used to be specific to military programs have now become commonplace, makes it possible for proliferation networks and countries to deceive the vigilance of authorities responsible for proliferation control. Finally, the appearance of suppliers capable of and wishing to transfer complete systems and related technologies to potential purchasers is one of the factors that triggers setting up these new proliferation networks. In this respect, the case of North Korean ballistic exports is symptomatic in that it is integrated into a set of criminal activities designed to finance the nomenklatura[9].

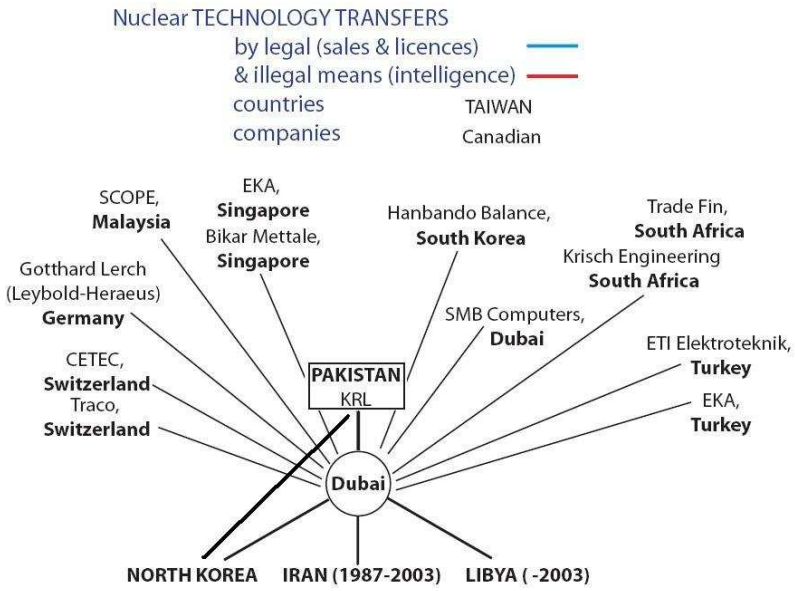
Thus, operations performed by the Khan network and adaptation of the Iraqi acquisition system illustrate trends in proliferation flows. Both are fairly extensive and their operations are sufficiently well known so that we can understand practical aspects of their operation and draw conclusions about the structure of this type of organization.

[7] We can talk about incentives and disincentives. See « *The Diffusion of Military Technologies and Ideas* », Edited by Emily O. Goldman & Leslie C. Eliason, Stanford University Press, 2003, p. 163.
[8] « Globalization and WMD Proliferation Networks: Challenges to US Security », Naval Postgraduate School, Conference Report, July 2005.
[9] These activities combine traffic in false currency, drugs and counterfeiting.

1.1 – Case studies

1.1.1 – Suppliers: The A. Q. Khan network

➡ **History**



The Pakistani acquisition network was formed in the 1970s so that Pakistan could develop its military nuclear program in order to match the test performed by India in 1974, and was based particularly on one of the figures in this program, namely Dr Abdul Qader Khan.

Suppliers, intermediaries and scientific and technical contacts encountered during the procedures aimed at controlling the fuel cycle and obtaining drawings for nuclear weapons, were personally linked to A. Q. Khan. These personal relations are undoubtedly one of the main characteristics of the Pakistani network. Thus, the Sri Lankan Buhary Seyed Abu Tahir (BSA Tahir), who appears to have been Khan's right hand within the network, had apparently met Khan for the project to supply air conditioning equipment to the *Kahuta Research Laboratory* (KRL)[10]. The other persons belonging to the network had also cooperated with Khan within the framework of the Pakistani nuclear program.

The use of this network for export/sale of nuclear technologies appears to have developed during the mid-1980s. At this time, Khan's organization was undoubtedly still integrated into a much larger assembly under the control of the Pakistani Government. Everything suggests that it was not until the mid-1990s that Khan progressively detached part of the organization, to work for his personal profit. This new private network, that BSA Tahir qualified as a ("*loose organization*"[11]), became permanently independent in 1999.

Therefore, the first known project in the Pakistani supply network was in the mid-1980s. At this time, Khan apparently had contacts with Iran for the supply of centrifuge drawings. The project was completed in 1994-1995 when A. Q. Khan made BSA Tahir responsible for transferring centrifuges from Pakistan to Iran through his company, the SMB Group, installed in Dubai. This transaction was worth 3 million dollars, and Iran paid for it by a cash payment in United Arab Emirate dirhams to BSA Tahir.

[10] See the report on the investigation carried out by the Malaysian Police Services. Press Release by Inspector General of Police, Malaysia, « In Relation to Investigation on the Alleged Production of Components for Libya's Uranium Enrichment Programme », Released February 20, 2004.
[11] Ibid.

Furthermore, contacts with Iraq were apparently made before the first Gulf War for the supply of weapon drawings and centrifuging technologies[12]. According to available information, there was no follow up to the first interviews between the Iraqi Intelligence Services (IIS) and Khan's representatives. However, a preliminary meeting was held in Greece at the end of 1990, during which an agent belonging to the network suggested using a Dubai intermediary for acquisition of some goods from the West. Financially, this agent requested a 10% commission for each acquisition made in the West, to be added to a fixed sum of 5 million dollars for the entire operation.

Contacts between the Khan Network and North Korea began within the framework of the official relation developed between Islamabad and Pyongyang at the end of the 1980s. Following the visit by Benazir Buttho to Korea in December 1993, cooperation appears to have materialized through the technology transfer for Nodong missiles to Pakistan. *Khan Research Laboratories* (KRL), then in competition with the *Pakistan Atomic Energy Commission* on the nuclear program, was central to relations with Pyongyang. Apart from the sale of a few tens of missile assemblies and at least one launcher[13], Pakistan obtained the transfer of know how, technology, and construction of an assembly site from the Communist regime. With North Korean support, Pakistan made its first flight test of the Ghauri missile on April 6 1998. According to revelations made by A. Q. Khan[14], his network started to deliver uranium hexafluoride (UF6), uranium enrichment facilities, as well weapon drawings to Pyongyang directly from Pakistan,[15] starting from 1997. KRL personnel also provided technical support at the request of North Korea. Even if these transfers were made outside government control, as claimed by the Pakistani authorities, there is no doubt they were made possible by the central role occupied by the KRL and Khan himself in ballistic cooperation. Furthermore, official Pakistani claims do not answer the question of the Pakistani counterpart for North Korean transfers.

Pakistan's economic situation became very degraded during the period concerned: low growth, high inflation (about 10%), high debt, reducing investments, low productivity[16]. It only began to improve starting from 2000-2001, under the influence of reforms initiated by Pervez Musharraf under pressure from the International Monetary Fund and the World Bank. In plain terms, Pakistan was not in a position at the time to finance ballistic acquisitions from a country that considers its programs as being a prime source of currency. Obviously, it is difficult to make a precise estimate of the amount of the

[12] D. Albright & C. Hinderstein, « Documents Indicate A. Q. Khan Offered Nuclear Weapon Designs to Iraq in 1990: Did He Approach Other Countries ? ».
http://www.isis-online.org/publications/southasia/khan_memo.html.

[13] Estimates vary between 12 and 25 missiles. Joseph S. Bermudez, « A History of Ballistic Missiles Development in the DPRK », CNS Occasional Papers No. 2, 1999, pp. 23-24.

[14] C. Braun & C. F. Chyba, « Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime », *International Security*, Vol. 29, No. 2, Fall 2004, p. 12

[15] Gaurav Kampani, « Proliferation Unbound: Nuclear Tales from Pakistan », February 23, 2004. http://cns.miis.edu/pubs/week/040223.htm
Note also the possible complicity of the Popular Republic of China in facilitating physical transfers: « *The high-capacity C-130 Hercules aircraft made numerous round trips to* Pyongyang *in the 1990s, both with and without Khan, presumably to deliver centrifuges and other nuclear parts. In each case the planes flew through Chinese airspace over* Xinjiang *and Chinese-controlled airspace in* Tibet *and* Qinghai*. Given the 2,000 mile range of the C-130, refuelling would have been required, almost certainly at* PLAAF *bases en-route.* »
http://en.wikipedia.org/wiki/Abdul_Qadeer_Khan#Development_of_nuclear_weapons

[16] International Monetary Fund, « Pakistan – Recent Economic Developments », December 1997.

transaction, but we might assume a unit price of about 4 million dollars per missile[17], giving a total of about 40 million dollars plus commissions for the transfer of technologies and installation of production facilities. Realistically, it can be estimated that the total amount might be about a hundred million dollars for which North Korea would have demanded fast and complete payment considering its own economic situation and the regime's clientelistic constraints. Considering everything, the principle of a barter transaction appears plausible, even though it appears likely that A. Q. Khan was paid a commission globally similar to that requested by him for a similar delivery to Libya[18].

Starting in 1997, Libya also contacted the Khan network to acquire uranium enrichment facilities for military purposes[19]. The first meetings in which BSA Tahir participated took place in Turkey, Morocco and Dubai. The Khan network initiated several operations to satisfy its customer's needs, starting in 2001:

- Delivery of 1.7 tonnes of uranium hexafluoride; the transport was done by air from Pakistan. This transaction was financially separate from the others.
- The supply of type P-1 and P-2 centrifuges, assembled or in kits. Two hundred P-1 centrifuges, two P-2 type centrifuges and several tens of components for type P-2 centrifuges were delivered directly from Pakistan.
- Construction of a manufacturing workshop for centrifuge components (Machine Shop-1001 project / 1001 project).
- The supply of drawings of nuclear weapons.

These operations were coordinated by Khan and their total amount was several hundred million dollars. One of them is particularly significant in that it used the network woven by Khan since the 1970-80s. The 1001 Project, for which BSA Tahir was the main organizer and treasurer, required the network to be capable of discretely transferring and building a manufacturing plant for centrifuge components in Libya, and also development of a long-term procurement capacity for the program. Two independent systems would be used for this purpose:

- One system involving several persons including a British national, Peter Griffin, was made responsible for purchasing machine tools and production means (vacuum furnace) in Europe, and providing training for Libyan technicians on use of these machines[20].
- The other system was organized around several members of the Tinner family, South African nationals who had participated in Pretoria's nuclear program, and companies in several countries, was to supply key components for assembly of the centrifuges. Some of these components including centrifuge casings, would be produced (based on drawings supplied by the network) by a Malaysian company *Scomi Precision Engineering* (SCOPE). Urs Tinner was seconded to SCOPE between April 2002 and October 2003, to assist with the manufacturing of parts to be

[17] « Seoul details N. Korea's Taepodong-2 ties to Iran, calls missiles main cash source », *East-Asia Intel*, August 9, 2006. The unit price of a Nodong system is estimated at 4 million dollars
[18] See below.
[19] Sammy Salama & Lydia Hansell, « Companies Reported to Have Sold or Attempted to Sell Libya Gas Centrifuge Components », Center for Nonproliferation Studies, March 2005.
[20] Press Release by Inspector General of Police, Malaysia, « In Relation to Investigation on the Alleged Production of Components for Libya's Uranium Enrichment Programme », Released February 20, 2004.

delivered to Libya through a Dubai company. The final destination of components made by SCOPE was the United Arab Emirates, within the framework of oil activities.[21]. For the needs of this operation, SCOPE needed to import large quantities of aluminum bars and cylinders from the Singapore subsidiary of Bikar Mettal. Interception of a cargo of components originating from SCOPE on board the German ship *BBC China* heading towards Libya on October 4 2003 led to dismantling of the operation. Companies managed by Khan's relations in Switzerland, Germany, Turkey and South Africa were also involved in procurement for the Libyan program.

➧ Organization of the Khan network

At the heart of the network, there was a series of trusted men that A. Q. Khan had met within the framework of the Pakistani nuclear program and the acquisition activities that he was managing. However, A. Q. Khan played the leading role in organization of the network, both as coordinator and technical authority. Everything suggests that he used the potential of KRL to give technical support to his network[22], in other words to be in a position to make complete proposals including control of the entire enrichment cycle. Similarly, Khan was able to use his contacts within the Pakistani administration so that he could export some sensitive products to his customers without restriction, and particularly centrifuges forming part of the nuclear program. It is difficult to believe that this activity could have been carried out without the political authorities of the country being aware of it.

The independence that Khan enjoyed within the framework of the Pakistani nuclear program and clandestine acquisition efforts may partly explain the ease with which the network was able to redirect its activities towards supply so discretely. However, it appears impossible that Pakistani security services [ISI] had not detected any indications about Khan's dealings. The North Korean episode suggests that the Pakistani military authorities had at best turned a blind eye in the interest of the country's strategic programs. Khan also appeared as the salesman for the network, and participated in several meetings with his customers.

The Sri Lankan Buhary Seyed Abu Tahir (BSA Tahir) appears to have become the main facilitator of network affairs, while the number of these affairs was increasing during 1994 and 1995. BSA Tahir was able to coordinate transactions generated by the Khan's enterprise through control of companies set up in Dubai, and particularly the SMB group of which he was the manager since 1985. His role in the network also included the creation and use of front companies, set up to facilitate the transit of goods to customers, and the management of various intermediaries and suppliers for the traffic[23]. Thus, BSA Tahir appears to have been responsible for remunerating companies working for the benefit of the network, both for companies that were instrumentalized like SCOPE, and companies familiar with the purpose of the operations. 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

[21] Ibid.
[22] Several of his close friends in laboratories were arrested in Pakistan in 2003.
[23] Sammy Salama & Lydia Hansell, « Companies Reported to Have Sold or Attempted to Sell Libya Gas Centrifuge Components », op. cit.

SCOPE, for an amount of 13 million dollars[24]. This role as the financial and logistics manager appears to be confirmed by his presence at meetings between Khan and customers of the network, and by his close contacts with other members of the network[25].

Depending on each project, other consultants were involved in the network, either to set up front companies or to supply equipment, or to perform a particular operation. However, these consultants do not appear to have played a permanent role in network activities, but rather to have been made responsible for performing a specific isolated mission. This is the case for Peter Griffin, firstly appointed to be responsible for SCOPE work for the benefit of the Libyan customer, and later replaced by Urs Tinner. For each operation, everything suggests that the Khan network was organized individually to satisfy the demand. Thus, Gotthard Lerch, who Khan had met in the 1970s in Europe, was apparently responsible for the Libyan operation and directly responsible for coordination of the South African branch[26].

Several companies also played a central role in the Pakistani network, either deliberately or unknowingly. Apart from the isolated involvement of some companies for specific projects, others appear to have made a direct contribution to operation of the network. Very generally, three types of companies can be identified depending on their role:

- Front companies, set up essentially in Dubai, have been used for acquisition of equipment from suppliers or intermediaries, dissimulating the final destination of the goods. For example, this is the case of *Gulf Technical Industries* and SMB. Apart from their occasional role in the network, these corporations have normal commercial and/or industrial activities and most of them have been in existence for several years[27]. The creation of "empty shells" for specific operations is often mentioned, but no precise data is available to conclude whether or not they are used systematically.
- Intermediaries, including companies and persons, play a central role in network procurement. The main intermediaries in the Khan network established in Europe, Asia and Africa, had the task of acquiring components or machine tools from European suppliers and forwarding them as far as Dubai front companies. In the Libyan case, a South African intermediary, Gerhard Wisser, linked to acquisition activities for Pretoria's former nuclear program and with historical relations with Khan, also participated in obtaining some key components from a South African corporation[28]. These professional intermediaries were remunerated through sales made through the network and everything suggests that they carried out other activities of the same type.
- Voluntary or involuntary supplier companies. Many companies supplied the Khan network with technologies and goods necessary to satisfy the needs of its customers. It is striking to observe that although some are set up in countries that do not have

[24] Michael Laufer, « A. Q. Khan Nuclear Chronology », Carnegie Endowment for International Peace, Proliferation Brief, Vol. 8, No. 8, September 2005, p. 7.
[25] « Companies Reported to Have Sold or Attempted to Sell Libya Gas Centrifuge Components », op. cit.
[26] « Network of Death on Trial », *Der Spiegel*, March 13 2006 (translation http://service.spiegel.de/cache/international/spiegel/0,1518,druck-405847,00.html)
[27] For example, SMB was created in 1980 by BSA Tahir's father, and is carrying out activities in the field of information technologies
[28] « Companies Reported to Have Sold or Attempted to Sell Libya Gas Centrifuge Components », op. cit.

good control over their exports, others in Europe or through their subsidiaries were used efficiently for the needs of the system. In particular, intermediaries were able to acquire high performance machine tools in Europe with impunity and were capable of having technicians in client countries trained in how to use these machines[29].

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[30] and/or front companies. Thus, the contract between SMB and SCOPE appears to have been financed conventionally, probably through letters of credit[31] or bills of exchange[32].
- Cash transactions[33] 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[34].

It appears that three pathways were used for management of material flows resulting from the network operations:

- Direct delivery of centrifuges and parts originating from Pakistan's stock and uranium hexafluoride, from Pakistan and by national means; in this case, the operation coordinated directly by Khan involved the use of a ship sailing under the Pakistani flag or a Pakistani civil or military aircraft[35].
- Indirect delivery from Pakistan through Dubai: in this case, the equipment was transferred in Dubai from a ship chartered in Pakistan to a ship flying the final destination flag. This ship made the delivery to the customer without the risk of exposing him or exposing the network.
- Indirect delivery by a supplier through Dubai; this case is different from the previous case in that the shipper did not know the final destination of the goods and used any transport means available to him. Once in Dubai, the load was transferred to a ship flying the flag of the Customer state that made the final delivery.

➡ Network operation

The A. Q. Khan Company appears to have always operated on the principle of a direct initial contact between the network leader and his customers. Once contacts had been made and main principles had been defined (amount of the operation, nature of

[29] See the Malaysian police investigation report
[30] Intermediaries have been remunerated, probably through industrial contracts
[31] Letter of credit: commitment by the issuing bank to make a payment to a supplier at the request of an order giver, on presentation of documents certifying that the goods have been shipped or a contract has been executed.
[32] Bill of exchange: document that the beneficiary submits to the creditor, and by accepting it the creditor orders his bank to pay the amount indicated on the defined due date.
[33] Press Release by Inspector General of Police, Malaysia, « In Relation to Investigation on… », op. cit.
[34] « Network of Death on Trial », *Der Spiegel*, op. cit.
[35] Press Release by Inspector General of Police, Malaysia, « In Relation to Investigation on… », op. cit.

supplies), Khan appears to have left his main associates responsible for operational implementation.

However, there is a significant difference in the development of the Iranian and the Libyan contracts. In the case of the Iranian contract, KRL's role appears to have been more central, particularly through the exclusive supply of goods and technology transfers directly from Pakistan. In the case of the Libyan contract, although KRL continued to play a role, operational management of technology flows and financial exchanges was delegated to a particular branch of the network. This change is probably related to Khan's personal situation and at least partial recovery of his activity by the military authorities of the country after Musharraf took power in 1999[36]. However, it appears clear that Pakistani intelligence services were aware of KRL's actions, or even that they supported them at least until the 1998 nuclear test, with the blessing of part of the political and military establishment[37]. In fact, despite the fact that information about Khan's actions appeared in the middle of the 1990s, particularly UNSCOM's discovery of an Iraqi internal document about the existence of a contact between Baghdad's nuclear program and Khan in 1996, the Pakistani Government waited until 2003 before it investigated the network. Its support was a crucial element in assuring continuation of network operations in the same way as specific measures taken by Khan to dissimulate flows (financial and physical) generated by him, and the confidentiality of contacts with his customers.

The basic business of the network was above all the supply of a complete proposal for enrichment of Uranium for military purposes. This offer was obviously supplemented by access to drawings of weapons compatible with the fissile material, and the possibility of obtaining uranium hexafluoride to supply the enrichment cycle. Furthermore, know how transfers related to work on uranium metal[38] are sometimes mentioned.

One of the specific features of this network is that the proposed supply is structured by setting up a complete service varying from the technical requirements specification to final delivery of a turnkey nuclear capacity. It thus corresponds to the very structure of the demand and its organization[39], in other words, the desire to dependably acquire a complete reliable capacity at low cost. However, this specific feature is largely due to Khan's personal career and the manner in which the Pakistani nuclear program was organized. It appears that tolerance of Pakistani authorities towards A. Q. Khan's activities and the operational method selected to acquire goods and technologies for the national program, facilitated the emergence and consolidation of a private activity.

[36] In particular, his elimination from KRLs' management in March 2001. Gaurav Kampani, « Proliferation Unbound: Nuclear Tales from Pakistan », February 2004.
« *In the face of strong U.S. criticism, the Pakistani government announced, in March 2001, that Dr. A. Q. Khan was to be dismissed from his post as Chairman, KRL, a move that drew strong criticism from the religious and nationalist opposition to the President of Pakistan, General Pervez Musharraf. Perhaps, in response to this, the Government of Pakistan, instead, appointed Dr. A. Q. Khan to the post of Special Science and Technology Adviser to the President of Pakistan with a ministerial rank. While this could be presented as a promotion for Dr. A. Q. Khan, it removed him from hands-on management of KRL and gave the Government of Pakistan an opportunity to keep a closer eye on his activities* ».
http://en.wikipedia.org/wiki/Abdul_Qadeer_Khan#Investigations_into_nuclear_proliferation
[37] Ibid.
[38] Michael Laufer, « A. Q. Khan Nuclear Chronology », op. cit.
[39] See below (Iraqi network).

Therefore, we can be concerned that clandestine acquisition networks in proliferation countries could one day become potential suppliers of the same type of proposed supply.

1.1.2 – Procurement: The Iraqi acquisition network (1991-2003 period)

➡ History and developments

The Iraqi technology acquisition system was set up starting from 1991 particularly to supply the country's non-conventional weapons programs, and was extended and became more complex to adapt to the changing context created by the development of the oil for food system.

Despite the embargo imposed by the United Nations, starting in 1996, the Iraqi acquisition system exploited the source of income from its oil sales within and outside the oil for food program, but also the partial opening of its market to imports to finance its operations and thus extend its suppliers network. This network includes private companies, intermediaries, banks and voluntary and involuntary suppliers, and also governments remunerated through the oil supply protocol[40].

Essentially, Iraqi acquisition attempts starting from 1991 related to ballistic missiles and aerobic missiles.

The period from 1991 to 1996 was marked essentially by contacts with companies set up in three countries, namely Romania, the Ukraine and Jordan[41]. While Romania and the Ukraine were used by Iraq as sources of technology and goods, Jordan was useful mainly as a turntable for financial and physical flows generated by acquisition activities.

Contacts with the Romanian company Aerofina apparently began in 1994 with meetings with experts in the guidance and navigation field so as to assist the Iraqi missile program based on modification of the SA-2. Deliveries of equipment through Jordan, particularly test means for missile gyroscopes began in Autumn 1994 but were temporarily interrupted in 1995 and then permanently stopped in 1998 after UNSCOM[42] discovered this operation. The Military Industrialization Committee (MIC) apparently also initiated contacts starting from 2001 through intermediaries and front companies, with the Romania Uzinexport Company for acquisition of equipment necessary for the production of magnets that could be used for manufacturing centrifuge bearings. Apparently, the agreement(s) signed between MIC intermediaries and the company related to support for manufacturing of magnets in Iraq. The total amount of the transaction paid for by a combination of cash funds and letters of credit was apparently 4.6 million dollars[43].

Cooperation with the Ukraine apparently began in 1995 through official visits combined with the supply of equipment by Ukrainian companies for an estimated amount of 140

[40] Baghdad signed clandestine oil supply protocols with its neighbors Syria, Jordan, Turkey, Yemen and Egypt. These protocols were a primordial source of income for Iraq's clandestine acquisition system.
[41] Iraqi Survey Group Final Report, September 30, 2004, p. 87.
[42] Ibid, p. 88.
[43] See below, for the financial organization of the Iraqi acquisition system

million dollars for the 1995-2001 period[44]. Cooperation related particularly to inertial guidance questions through contacts between Yuri Orshansky, Manager of the MontElect Company and Al Karama site managers. These contacts were also materialized by the transfer of complete SA-2 systems and components of this missile in 2001 through ARMOS, a front company belonging to MIC and set up in Russia[45]. Thus, Iraq apparently acquired 300 Volga[46] engines through MontElect and signed a contract for the construction of a propellant production site, and initiated contacts for the development of a ground test bench.

The involvement of Jordan (or Jordan-Iraqi) companies (banks, front companies-brokers) in the Iraqi acquisition system began in 1991 and continued until 2003. Jordan was used as a turntable for imports of equipment, financing source through the bilateral commercial protocol and intermediary for financial operations for the Iraqi network. The Iraqi Al Eman group[47], one of the main intermediaries of Iraqi secret services, organized material flows from Jordan, including the transport of goods to the final destination. In particular, its Jordan subsidiary apparently managed the acquisition of components for the Al Samoud program and various dual-use goods in the domain of navigation and propulsion, including GPS receivers, and gyroscopes. Financially, several Jordan banks and particularly the National Bank of Jordan, were used both to finance the acquisition activity of Iraqi intermediaries, and to collect illegal funds from the sale of oil. Until 1996, 95% of Iraq's acquisition activities were controlled by Jordan banks, this percentage dropping to 30% after the oil for food system had been set up.

Starting in 1996, Iraq broadened its range of suppliers by diverting the oil for food system to increase available financing.

Syria gradually replaced Jordan as the turntable for Iraqi traffic. Starting from the signature of the commercial agreement in 2000, Iraq signed contracts under this protocol for an amount of 1.2 billion dollars[48]. Iraqi imports were then managed directly by a Syrian company, SES International, itself in contact with front companies forming part of the Iraqi acquisition network and particularly the Al Basha'ir group under the control of the MIC, or directly with Iraqi ministries or bodies. To a lesser extent, Turkey also became an essential source of income for the Iraqi network, starting from 2000. The various traffic generated about 1 billion dollars per year with its neighbor, which was sufficient to supply the network's accounts in the different banks in the region, in Lebanon, Turkey and Jordan.

Starting from when the oil for food system was set up, the Iraqi network appears to have woven new links with several Chinese companies for the supply of components in the guidance domain. In particular, the Chinese NORINCO Company appears to have been contacted starting from 2000 for the supply of gyroscopes for the Iraqi missile program. Even if many contacts apparently led to nothing, the relation between the Iraqi network

[44] ISG Final Report, p. 89.
[45] See below.
[46] This is the SA-2 engine. Iraq recognized having acquired these engines in the document submitted to the UNMOVIC in December 2002.
[47] See the Duelfer report (first ISG report), p. 88. http://www.lib.umich.edu/govdocs/pdf/duelfer1_db.pdf
[48] Note that not all these contracts necessarily apply to illegal acquisitions. According to data collected by the ISG, 186 million dollars were set aside for this type of operation. ISG Final Report, p. 94.

and some Chinese companies appears to have been successful in terms of projects.[49]. Even if some Iraqi delegations came into contact with potential suppliers directly, flows were managed by Iraqi intermediaries located in the Near East and in Asia to facilitate export of equipment to Baghdad.

Due to the relationship set up with the Bulgarian JEFF Company starting from 1998, the Al Basha'ir group and SES International appear to have been able to supply the Iraqi network with various goods necessary for development of the missiles program and particularly machine tools, and propellant components.

The creation of the Iraqi-Russian ARMOS *joint venture* in 1998 provided the Iraqi acquisition network with the means of developing its links with Moscow. Baghdad apparently also used its embassy in Moscow to transport the goods and funds between Russia, Syria and Iraq, and in particular Iraq also used the ARMOS Company to set up relations with the Russian Rosoboronexport Company that had transferred goods to Iraq using false final destination certificates produced by the Syrian authorities. Most contracts signed between ARMOS and Russian companies dealt with technical support in the missile field[50]. Thus, the TECHNOMASH Company[51] was apparently awarded contracts to supply support in the field of navigation and structures, and for the construction of a test bench for engines. ARMOS also negotiated contracts for the supply of 280 Volga engines for Al Karama in 2002. These engines and other missile components were transferred from Poland through a Polish intermediary (Ewex Company) for the benefit of the Iraqi Al Basha'ir Company.

Among the various other contacts made by the Iraqi network after 1996, the contact set up in 1999 with North Korea is noteworthy. In particular, the MIC had attempted to acquire long-range ballistic missiles (Nodong type) and anti-ship missiles from the North Korean *Changwang Trading Company*[52]. Several contracts were signed between this company and Iraqi entities related to the Samoud program in 2000 and 2001, particularly dealing with the supply of North Korean components. Payments were made directly to the North Korean Embassy in Damascus through the Syrian SES International Company, using funds obtained through the Syria-Iraq commercial agreement[53].

Indian, Belarus, Taiwanese and Egyptian companies also participated in the supply of components to the Iraqi network. In most cases, use of non-Iraqi banks as relays and cash payments by Iraqi diplomatic personnel formed the basis for management of financial flows generated by Iraqi acquisitions.

➡ Organization of the Iraqi network

Saddam Hussein was at the highest level of the Iraqi acquisition system, controlling the budget dedicated to illegal activities. This role included particularly the production of commercial agreements with neighboring countries that acted as sources of income and

[49] ISG Final Report, pp. 102-103.
[50] ISG Final Report, p. 109.
[51] One of the main Russian design offices for space systems.
[52] One of the Korean entities sanctioned by the American administration for acting as an intermediary for exports of missile technologies from North Korea.
[53] ISG Final Report, p. 110.

as turntables for flows to and from Iraq. Although two bodies (the Presidential Secretariat and Diwan) actually managed financing allocated to the projects of requesting organizations (secret services, MIC), the final decision whether or not to commit funds was made by Saddam Hussein.

By setting up bilateral commercial agreements after adoption of the oil for food system, the Iraqi regime could develop its acquisition network in signatory countries. Thus, Baghdad financially maintained a series of industrial and financial intermediaries directly managing acquisition operations. Iraqi companies already engaged in this type of activity before 1996 were able to set up directly controlled branches in other countries acting as relays for needs expressed by customers and tools for the management of financial and equipment flows.

These front companies, some of which were set up in the early 1990s either by the MIC or by Iraqi secret services, formed one of the driving forces of the Iraqi system and handled hundreds of operations and actually coordinated acquisitions.

The Al Basha'ir Trading Company was thus one of the main Iraqi acquisition companies. It was set up in 1991 under the control of the MIC and probably the Iraqi secret services, and broadened its field of activities by setting up several regional offices in countries acting either as suppliers or as turntables to the network. Thus, starting in 1996, the company controlled more than 50% of all activities carried out under the auspices of the Iraqi-Syrian agreement[54], in other words a large part of the Iraqi acquisition activity. In particular, this company was to participate alongside SES International and ARCOM, in negotiations with suppliers in Eastern Europe. Al Basha'ir also acted as an intermediary to Iraq for illegal oil sales, although this was not the core of its activity. According to the archives of the Iraqi SOMO oil company, its Jordan branch signed 198 contracts for the supply of oil products for a total amount of 15.4 million dollars. The MIC created the *Al-Mafakher for Commercial Agencies and Export Company*[55] in 2001, and carried out a few operations but its activity volume was less than the Al Basha'ir Company.

Apart from the acquisition activity carried out by Al Basha'ir, the Iraqi regime encouraged the creation of multinational companies under the control of Iraqi citizens. Their links with security services made them ideal tools for serving the interests of the Iraqi acquisition network in other countries. Thus, the Al Eman family company that had subsidiaries in Dubai and also in Amman, played a special role in financial and equipment traffic from Jordan. By drawing upon accounts supplied through illegal oil sales, its subsidiaries managed various aspects including the logistics for flows towards Iraq. Commercial attaches (members of the services) in Iraqi embassies were in permanent contact with members of the Al Gaood family[56] who managed the conglomerate and acted as intermediaries during preliminary contacts with potential suppliers.

Since the end of the 1990-1991 war, the Iraqi Intelligence Services (IIS) facilitated the acquisition network operations. Starting from 1997, cooperation with the MIC optimized activities. While the MIC's responsibility was to financially maintain the

[54] ISG Final Report, p. 73.
[55] ISG Final Report, p. 77.
[56] ISG Final Report, pp. 87-89.

network of intermediaries and front companies, both by deciding upon allocated funds and specifying needs, the IISs were to use their agents as:

- Couriers for particularly sensitive transfers through generalization of the use of diplomatic positions and the diplomatic case to transport property acquired through the network or cash funds intended for intermediaries or suppliers. Some acquisition operations were also managed completely by IISs under the technical control of MIC[57].
- Intermediaries for setting up front companies for the network in other countries; these corporations were used when required to approach potential suppliers and to carry out transactions with them. They could occasionally export goods to and from the turntables in the network (Syria and Jordan).
- Facilitators for the entry of contraband equipment into Iraq; setting up of IIS units at the main entry points to Iraq or in transit ports, to facilitate entry by land or sea of goods acquired through the network[58]. In particular, these units were made responsible for avoiding inspection of loads acquired through the network and entering the Iraqi territory, using any possible methods.

The Iraqi regime had accumulated 10.9 billion dollars[59] of illegal income between 1990 and 2003, by four means:

- Signature of bilateral commercial protocols with its main neighbors and allies; the main source of income (about 8 billion dollars) was based on the export of oil products outside the oil for food program.
- Extra costs applied to the sale of oil under the "oil for food" system; starting from June 2000, the Iraqi regime applied a "tax" of 25-30% per barrel to oil sales, through the SOMO State Company. This extra cost was paid by customers either through transfers to SOMO's accounts or in cash to Iraqi diplomatic missions[60]. The amount collected using this system was 265 million dollars.
- An under-the-table system applicable to imports within the framework of the "oil for food" program; companies providing goods to Iraq were expected to pay a percentage of the contract (about 10%) to the Iraqi network. The amount was deposited in a blocked account until payment for the delivery, and was then transferred to an Iraqi account or to a front company account. This method generated about 1.5 billion dollars of income.
- Sale of oil products to private companies outside the framework of the "oil for food" program. This activity generated about 1.2 billion dollars between 1991 and 2003. Payments were made in cash, by transfers to Iraqi accounts in other countries or through the delivery of goods.

In financial terms, the Iraqi network appears to have used three methods to conceal the destination and purpose of cash transfers:

- The first method was to finance some transactions by payments in cash made by the IIS agents located in supplier countries. The goods thus obtained could then be delivered through the diplomatic channel as far as Jordan or Syria and then transferred as contraband to Iraq. Money was transferred from these countries to

[57] ISG Final Report, p. 80.
[58] This was the case particularly at entry points monitored by inspectors of the oil for food program.
[59] ISG Final Report, p. 23.
[60] Ibid, p. 32.

foreign countries using diplomatic cases to prevent detection of movements between banks[61].

- The second method, used essentially after 1999, was payment through front companies with accounts in banks in nearby countries (Jordan, Syria). Payments were made by bank transfers (letters of credit) on delivery of the good(s) concerned. The accounts of front companies were supplied by the Iraqi Central Bank through credits in the national banks of turntable countries. This is how a network of several tens of international accounts developed, in the names of private individuals and under the financial control of the Central Bank, so as to receive funds originating from illegal sales of oil products and to manage their use by Iraqi bodies working at the heart of the network. Starting in 1996, some of the money from the oil income traffic was transferred to Iraq manually by delegations of the Iraqi Central Bank so as to pay foreign suppliers directly using the first method.
- Finally, Iraq engaged in barter, in other words financing of acquisitions through the distribution of drawing vouchers on oil production. This system appears to have been used occasionally to supplement cash financing. However, the drawing vouchers system was used more widely to corrupt foreign officials, including for the activities of the acquisition network.

➧ Operation, distribution and understanding and control of purchased goods

The Military Industrialization Committee (MIC) was the main beneficiary of activities performed by the Iraqi acquisition network.

The MIC received equipment requests annually from one of the 51 business places under its control within the framework of the budget process, and issued calls for bids to its intermediaries. MIC import commissions under the control of the technical department were made responsible for selecting suppliers based on received calls for bids, particularly at the Baghdad Annual Trade Fair. Apart from its own resources, for which the illegal part was deposited in foreign accounts in Jordan, Syria and Lebanon, the MIC could also draw upon the funds of the Iraqi Central Bank in order to honor its contracts.

However, part of the procurements was coordinated with IISs under the responsibility of the MIC Research & Development Office. In this more informal context, meetings could be organized between the potential suppliers and engineers in the user's business place[62].

The Iraqi acquisition network supplied programs, particularly the missile program, with components that were sometimes critical for their development. For example, the purchase of several hundred Volga engines effectively satisfied development needs for the Samoud program and the constraint imposed by the Special Commission[63].

[61] ISG Final Report, p. 46.
[62] ISG Final Report, p. 68.
[63] In 1996, the Commission had banned Iraq from using engines from its SA-2 fleet for development of the Samoud.

However, despite some technical successes, the efficiency of the entire network is uncertain[64]. The system set up by Iraq increased the number of intermediaries and administrative participants, but did not leave much scope for users to make technical assessments of proposals. Everything suggests that business handled entirely by the IISs must have led to the acquisition of goods that were not useful for the programs considered. The initiation of a genuine coordination between the MIC and the IISs starting in October 1999 undoubtedly corrected this weakness, at least partly.

Operation of the system was also made possible by complicity of the governments of some of Iraq's neighbors that benefited from commercial agreements and that knowingly facilitated flows generated by acquisition efforts. Thus, the systematic use of false documents (end use certificates, customs declarations and loading declarations) and dissimulation of the final user were made possible by the existence of these preferred links. This method enabled the Iraqi network to obtain required goods from voluntarily or involuntarily participating companies, by circumventing export control systems.

Similarly, cooperation with banks in some of these States was essential to facilitate cash movements between Iraq and its customers. This cooperation involved firstly central banks, but also commercial banks. Thus, the Iraqi Rafidian bank that has branches in several countries in the Gulf region and in Europe, acted as intermediary between the Iraqi Central Bank and its corresponding banks, and banks of which Iraq was client[65].

The Iraqi network was highly structured and modulable, and successfully used available resources badly controlled by the United Nations, to provide means for the country's programs despite a severe embargo. Although some aspects of its operation are probably unique, the model is nevertheless undoubtedly valid for other acquisition networks, particularly networks based on illegally acquired funds. As an illustration, the North Korean network must be fairly similar to the Iraqi network, particularly financially with the use of relay banks designed firstly to launder money derived from various traffic, and to finance purchases. Thus, freezing of North Korean credits deposited in the Banco Delta Asia bank, that led North Korea to transfer funds to other accounts in Europe and Asia[66], appears to have correspondingly affected the North Korean acquisition network and some Pyongyang illegal traffic. The systematic use of diplomatic channels for cash movements also appears to form part of the arsenal of means used by North Korea to supply its acquisition network.

1.2 – Modeling of proliferation networks

1.2.1 – Supplier networks

➡ **Functional analysis**

If it is to be able to operate, a supplier's network must be capable of offering its customers the product(s) best adapted to their needs and within their budget, but must

[64] For example, the purchase of gyroscopes for submarine-launched ballistic missiles in 1995; these components were unusable for the Iraqi missiles program.
[65] The Rafidian bank had branches in Lebanon, Jordan, Egypt, Kuwait and even in the United Kingdom.
[66] « N. Korea now channelling overseas cash via Austria after U.S. sanctions on Macau bank », *East Asia Intel*, December 21 2005.

also be capable of delivering it discretely. This is one of the key capacities of a suppliers' network, together with a series of optional services, for example such as setting up technical support during the project definition phase or on-site to help define the need[67].

Thus, essential functions necessary in a suppliers' network can be identified:

- Engineering: in other words the capability of making a proposal corresponding to the customer's need. Existence of this function is the necessary condition for the network to exist, in that it is capable of proposing a product or a service. This product or service may be primary (a specific component) or it may be complex (a complete proposal, knowledge or know how). The engineering function may also be provided through the network itself, subcontracted to suppliers (voluntary or otherwise) or may be shared between external suppliers and part of the network.
- Logistic: Including management of production or acquisition of the goods concerned and their routing to the customer. For some projects, routing can be done partly by the network itself and partly by the customer[68]. Similarly, production can be subcontracted to companies working for the network, as was the case for SCOPE. In any case, coordination with the customer and internal flows management, are key functions for the network.
- Financial: This concerns the capability of managing financial flows, both within the network to pay intermediaries and suppliers, and outside the network. The network must be capable of receiving payments for transactions and distributing them to the various persons concerned, while camouflaging operations. This means that it is capable of laundering money received from its customers, and also using its funds to acquire goods for its customers.

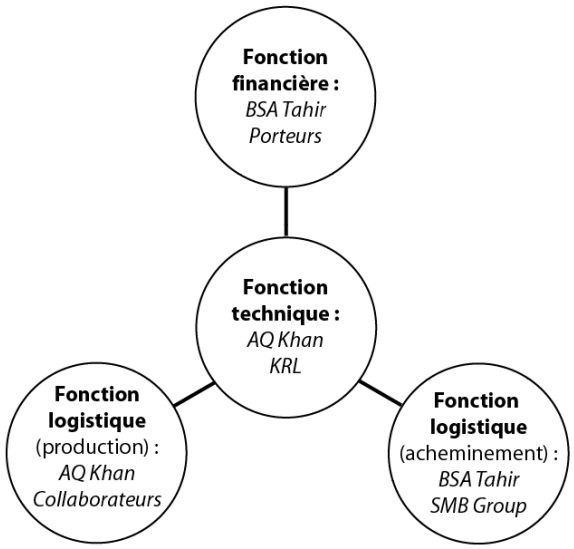
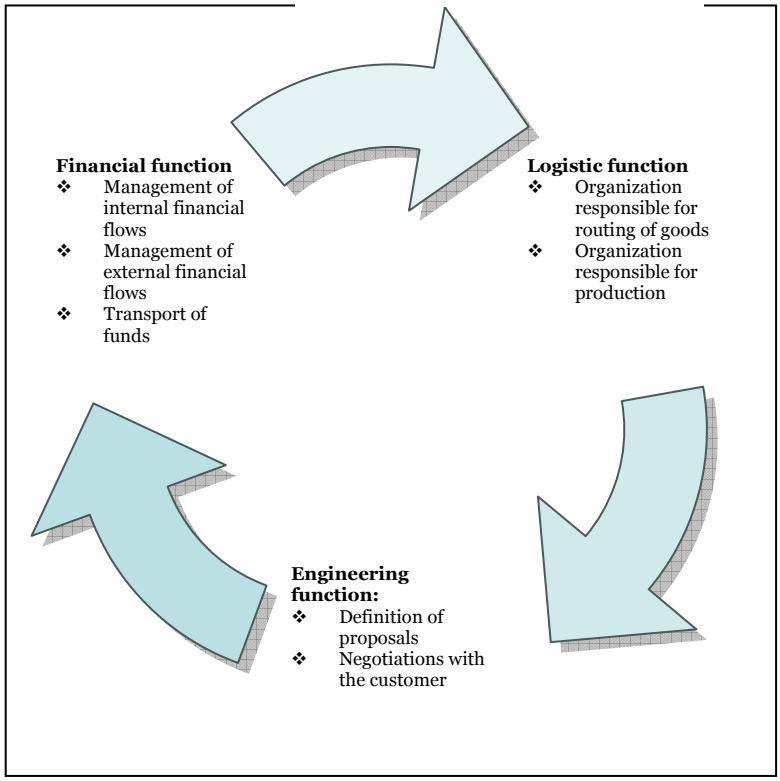


Fig. 1 **: distribution des fonctions assurées par le réseau Khan**

[67] This is the « advantage » of the Khan network.

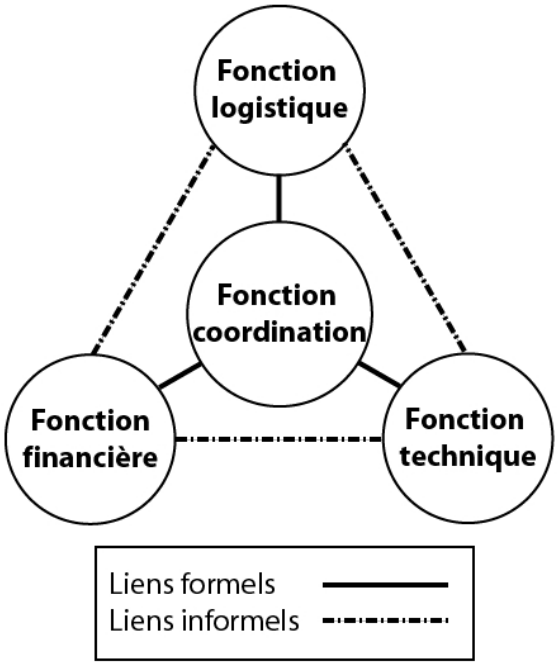
[68] Particularly if the customer manages his own acquisition network. For example, in the case of Khan's proposal to the Iraqis, Iraq would undoubtedly have wanted to control part of the routing.

Fig. 2 : Distribution of functions
in a State network



Interactions between these functions determine the basic structure of the network. Considering the case the A. Q. Khan network once more, some functions are performed by a single person. Thus, BSA Tahir manages routings and financial flows, while A. Q. Khan and some intermediaries or associates are responsible for engineering and production aspects. However in this case, a single person is responsible for coordinating key functions. Although this centralized aspect makes the organization efficient provided that the key person is competent, it also makes the organization vulnerable to disappearance of this person. This weakness can be compensated if the central level includes one or several redundancies, in other works persons or an organization capable of performing the coordination function in the case of a failure.

Fig. 3 : **structure informelle (simplifiée)**



Networks structured around organizations rather than persons appear to be less fragile[69]. Due to their national nature, they also benefit from extra means in terms of routing and financial operations. In particular, they can transport goods with national means or they can benefit from diplomatic advantages. On the other hand, the structural weight imposed by the involvement of organizations can harm the overall efficiency. Therefore, coordination between engineering, logistic and financial functions may be a source of difficulty for the network, partly due to competition or even the lack of cooperation between the organizations involved. However, this difficulty appears to be less crucial for the operation of a suppliers network than it might be for an acquisition network.

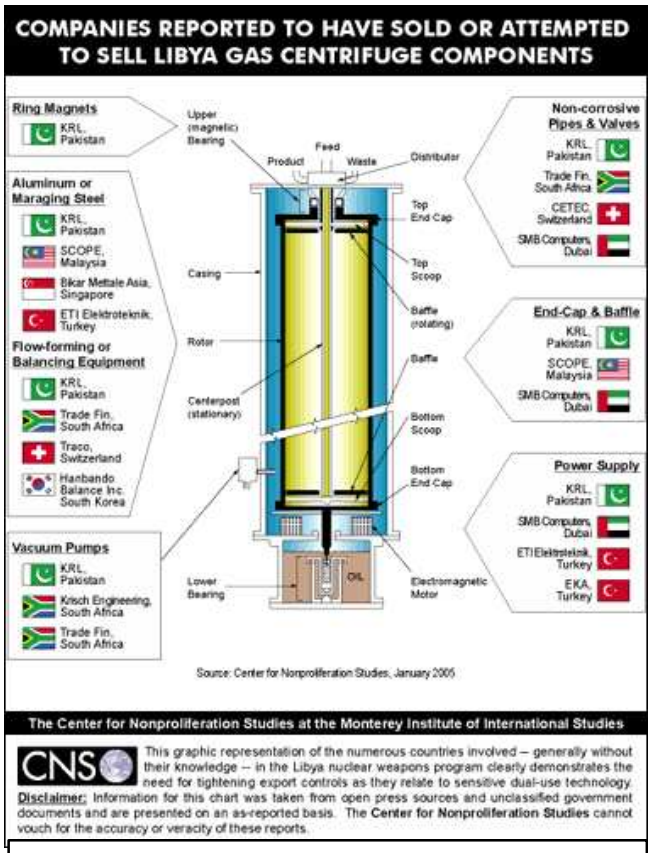
Therefore, two basic models could be considered for suppliers networks, corresponding to two different realities:

- A star model, *a priori* corresponding to a private or semi-private network (of the Khan type, fig. 1).
- A cyclic model, *a priori* corresponding to a national network (of the North Korean type, fig. 2).

Combination of the two models would be possible, that would correspond to the Khan network structure between 1992 and 1999, and in which organizations of the State concerned are involved with central control exercised by an individual. The existence of organizations with a more informal structure, in which each center is linked to the others, is noteworthy[70]. From a functional point of view, such a network appears relatively complex to manage. However, this type of network could be envisaged in a scenario of degrading cyclic or star networks, in which participants no longer coordinate at a global level, and instead create informal links between themselves. (fig.3). Such a configuration makes the network less vulnerable to the disappearance of the coordination authority or one of the functional centers than the basic cases described above.

[69] For example, this is the case for the North Korean network for the supply of missile technologies.
[70] Alexander H. Montgomery, « Ringing in Proliferation », *International Security*, op. cit., p. 170.

➡ **Overall organization: circumventing regulations, financial and logistic operations, strong and weak points**



Origin of the centrifuge parts proposed by AQ Khan Network to Libya
: (Source : Center for Non Proliferation Studies)

Regardless of its functional structure, the mission of a suppliers network is to deliver a product to its customers conforming with their needs. To do this, in some cases, it must be capable of acquiring goods for the benefit of its customer and routing them, possibly in addition to its own proposal. Thus, the Khan network purchased goods from various European, Asian and South African companies on behalf of its customers.

In order to control this type of operation, the network must be capable of contacting foreign companies and assuring that national authorities do not detect that their goods have been exported. Therefore in terms of organization, the network needs to search and use intermediaries with good knowledge of the local industrial fabric and aware of the weaknesses of the national export control systems. It is also essential that the network should include front companies that will be official purchasers and therefore need to transport goods to their genuine destination.

These front companies also act as transit points for goods that have been acquired by intermediaries, and must route them. Their physical location must be chosen such that they reexport the acquired goods without any or with only a minimal control on their transfer.

In order to dissimulate their destination in the most restrictive case, in other words in a country with an efficient control system, intermediaries and front companies need to set up a series of measures:

➡ False documents: in particular, false final destination certificates or even forged non-reexport certificates when required to obtain an export authorization from the country concerned. In some cases, these documents have to be countersigned by the national authorities of the country in which the front companie operates[71]. Complicity within the government is then necessary. Thus, for the supply of AS-15/Kh-55 cruise missile airframes by the Ukraine to Iran and to China through

[71] This is the case for sensitive military and dual-use equipment exported from the United States. Some European countries are beginning to demand this type of visa for dual-use or military equipment.

Russia, one or several civil servants in Rosoboronexport had signed final user certificates to obtain a Ukrainian authorization. The use of false cargo manifests to conceal the nature of the product is another solution to escape from the efforts of Customs and intelligence services.

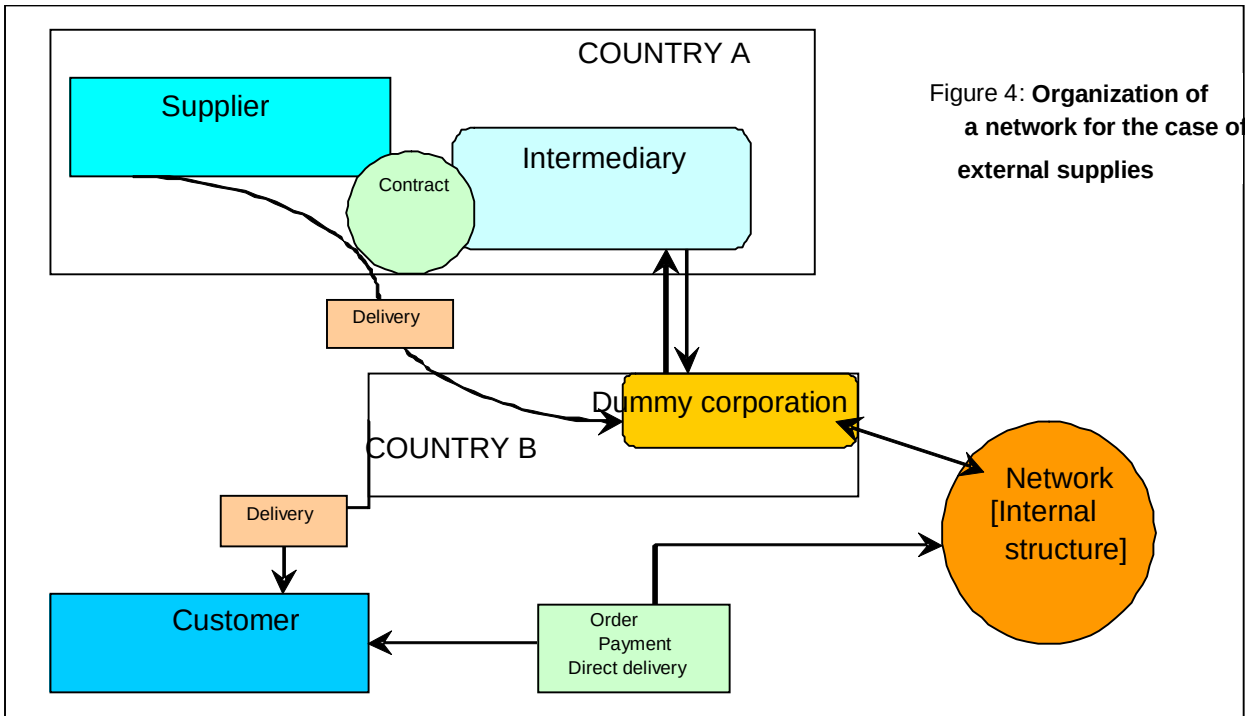


Figure 4: **Organization of a network for the case of external supplies**

- Selection of products, suppliers and transporters; the external part of the network (intermediaries and front companies) must select firmly dual-use goods wherever possible or goods that are not considered as being sensitive for the declared destination, so as to get around existing export control systems. Elementary components can also be chosen rather than complete subassemblies, the use of which is easier to determine. For example in the Libyan case, elements made by SCOPE that are useful for oil prospecting, could legitimately be sent to a Gulf company, in other words the network must be able to cover its activity by legitimate operations, making use of the diversity of suppliers and the location of front companies. Finally, the network selects transporters if the acquirer cannot use his own means.

If the network does not acquire equipment in other countries on behalf of its customers, it can minimize its external structure. It must then have its own routing means (assumed to be reliable) for goods and possibly for engineering support.

Capital and money movements are usually detectable, even in the case of direct bank transfers between national banks[72]. The main difficulty for suppliers networks is related to the volume of bank operations performed. Thus, a network using external players for some of its activities needs to perform a large number of financial operations, unlike an

[72] Automation of bank transfers led to setting up a secure international network activated by the SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) Company used by 7 800 financial institutions in 202 countries. SWIFT is centralized in Belgium and opened a back door to the CIA to check flows after September 11 2001.

organization providing its own production. There may be several operational choices for managing these flows:

- Perform as many operations in cash as possible; however, the use of currency introduces the problem of reinjecting this currency on the market, in other words its laundering. Some countries have introduced rules limiting the amount of cash payments[73], which should prevent networks from making cash payments to any suppliers[74]. In this case, considering the size of the financial flows involved, (in millions of dollars[75]), this market cannot be organized solely through currency transfers. On the other hand, cash payment for part of the network, particularly intermediaries or cooperating companies, would appear to be feasible.
- Use of a network of banks and financial institutions; the objective for the network is to place some of its financial resources in several banks or financial institutions that will receive payments and manage financial flows that will supply the various players. Thus, Pyongyang appears to have distributed income generated by its illegal activities in several Asian, European and American banks[76]. For some networks, it is also possible to set up financial institutions in other countries under their own control, with the exclusive role of managing their credits, paying suppliers and receiving payments from customers. Such a solution (similar to that set up by Iraq through the Rafidian bank) has the advantage of limiting the risk of credits being frozen and enabling illegal operations to be carried out without the risk of detection by financial control services.

[73] « Laundering continues despite increased vigilance», *Le Monde*, May 23 2006.
[74] Suppliers who do not form part of the network.
[75] Apparently the Khan network generated profits of a few hundred million dollars.
[76] « U.S. insists sanctions on N. Korea are having worldwide 'ripple effect' », *East Asia Intel*, April 12, 2006.

LAUNDERING AND "DIRTYING" OF MONEY IN PROLIFERATION

1. Money laundering

Definition[77]

Money laundering is one element of financial criminality techniques. It is the action of dissimulating the source of money acquired illegally (in our case the traffic of proliferation products prohibited for export) to reinvest it in legal activities. It is an important step, since without laundering, these companies would be unable to have proliferation networks as customers (the fruit of these illegal sales has to enter their accounts) and they could not use large amounts of this income without being identified.

There are usually several steps that occur in the laundering process; **investment** of amounts in financial products, **stacking** of intermediaries to loose track of the origin, finally **reinsertion** of funds into the legal economy.

Laundering methods in general and laundering methods used in proliferation

- **"Smurfing"**: bank deposits of small amounts in cash by several persons.
- **Bank complicity** (by a bank or an employee): for example the Rasheed Bank and Rafidian/Rafidain Bank for Iraq[78], the Delta bank and the branch of the Popular Republic of China Bank (national bank) in Macao for North Korea.
- **Purchase of goods in return for immediate cash payment**, but this is not possible if the State acquiring illegal weapons also wants a long-term relation with the supplier and does not want to be suspected.
- **Electronic transfer of funds**: if the CIA and the Treasury department of the SWIFT interbank network continue monitoring, this method is too risky because it leaves traces[79].
- **Amalgamation of funds in honest companies**: this method is too slow for proliferation countries that have immediate needs.

Although it is possible to struggle against state networks procuring "sensitive" products (fissile material, component included in the Zangger Committee list or the MTCR list), it is much more difficult to struggle against *a priori* legal operations (sales of sub-assemblies, spare parts for which the end use is not known), but which are actually traffic in dual-use goods.

[77] http://fr.wikipedia.org/wiki/Blanchiment_d'argent – http://en.wikipedia.org/wiki/Money_laundering
[78] http://www.globalsecurity.org/wmd/library/report/2004/isg-final-report/isg-final-report_vol1_rfp-anx-g.htm
[79] Terrorist Finance Tracking Program http://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication

2. Money "dirtying "[80]

Money dirtying is the contrary of money laundering.

While the main concern of suppliers paid by proliferation networks is to reinject illegal income into the official economy, the concern of a state that would like to develop illegal activities (purchase of parts prohibited for import, corruption) is usually the contrary, namely to generate concealed funds and dirty cash originating from money legally acquired.

The "Oil for food" program provides a wide variety of dirtying techniques used by Iraq: sets of commissions, piggy back by intermediaries (Embassy civil servants) during purchase operations …[81]

Typology of problems in each country:

- **Iraq, Iran, Libya** (oil exporting countries with hard currencies) already having "clean" money. The question of laundering does not arise for these countries since they already have clean money (income from oil). Therefore, they need to "dirty" some of this money that they use to buy goods on the world market or in western countries to conceal the user and the end use. There is no need to dirty money for purchases that they make in rogue countries (Khan Research Laboratory in Pakistan, North Korea, etc.);
- **North Korea** and other countries without hard currencies. Since the North Korean economy is very weak and only survives through the assistance of international aid (from South Korea, China and the world food program), the Pyongyang regime needs to acquire hard currencies before it can purchase imports. In the past, North Korea has done this by distributing false $100 notes and selling counterfeit such as Viagra, cigarettes and amphetamines in cooperation with Chinese gangsters[82].
- **Pakistan's** problems are probably the same; Pakistan is apparently willing to barter (with North Korea) to acquire technologies that it does not have (missiles) or so that Khan Research Laboratory can make a profit from its enrichment plants, or maybe to purchase them (?).
- Profit is one of the main motivations for **sub and trans-state semi-private networks** (like Khan) and sub-networks, therefore any honest or dishonest purchaser of their technology is acceptable.
- Several special features make the task of terrorists more difficult; if they have no "sanctuary" countries (like Iran), it is difficult for them to be supplied with missiles or radioactive materials. Furthermore, many suppliers might hesitate if the final destination were known. But on the contrary, ideology might also convince them to take greater risks and help them obtain goods through other cooperating suppliers sharing the same beliefs.

[80] http://fr.wikipedia.org/wiki/Noircissement_d%27argent
[81] http://en.wikipedia.org/wiki/Iraq_Survey_Group – http://www.globalsecurity.org/wmd/library/report/2004/isg-final-report/
[82] http://www.timesonline.co.uk/article/0,,2089-2261782,00.html

- Individuals alone:
  Eg: Gotthard Lerch[83]
- "Risk" countries that could illegally export proliferation technologies. Apart from Pakistan and North Korea already mentioned, Russia and China could be worrying.
  Russia: not much business discovered (in the traffic of radioactive materials) despite the possibilities, the reputation of Russia and fears (fantasies?).

For a supplier network, the ideal situation would be to be able to sell products wanted by its customers without the need to use brokers and external suppliers. The network would then have almost complete control over all flows generated by its traffic, and limit risks of detection and dismantling. However, this is not the case for known examples of supplier networks (North Korea, Khan). There are apparently two reasons that could account for this fact:

- The private nature of some networks; this is the case for the Khan network after 1999 that obliged them to acquire some goods in other countries to satisfy their customer's demand; the specific nature of these networks was also to propose a complete offer (from technologies to the production cycle). Since they are not necessarily capable of producing all necessary elements internally, external acquisition is essential (in the form of subcontracting).
- The dual nature of some networks; supplier networks are often also acquisition networks set up to satisfy national needs[84]. Existing structures for acquisition activities also manage the export activity. Therefore they need to generate larger flows and rely on more extensive international networks than if they only managed export activities.

➧ Determination of applicable criteria for making a judgment on vulnerabilities of a suppliers network

If it is to be efficient and durable, a supplier network should have three essential characteristics:

1. Discretion: particularly to escape detection by organizations responsible for monitoring suspicious movements of goods and capital: customs, intelligence agencies, police.
2. Efficiency and "affordability": to be capable of satisfying customer needs[85] at relatively accessible/affordable costs for customers, while assuring that the operation is cost effective for the supplier.
3. Resilience: the network must be able to continue operating if part of its means are eliminated or are no longer available.

[83] http://www.newyorker.com/online/content/?060807on_onlineonly
[84] This was the case of Khan before 1999 and of North Korea.
[85] Meaning that customers have to be known and contacted, so that their needs can be understood.

To judge on the vulnerability of a supplier network, in other words the possibility of permanently or durably neutralizing it, it is important to analyze what are its minimum conditions for operation. Therefore, it appears important to determine a set of elementary criteria to characterize the organization.[86].

The first is the **size and extent of the network**; the number of persons, organizations and companies involved in the network. The largest networks have the advantage that they facilitate a larger range of acquisitions, which increases their efficiency. On the other hand, smaller networks are less detectable and their operations are more discrete since there are fewer of them. However, they are more vulnerable to neutralization actions in that they have very little redundancy or none at all.

The second applicable criterion is the **functional concentration of the network**; the number of functions performed by one or a few units in the network. Thus, to the best of our knowledge, some functions in the Khan network were performed by a few persons. This is true particularly for network coordination and engineering functions, in which *a priori* only a handful of persons had any responsibilities[87]. For example, BSA Tahir worked as a coordinator for logistic and financial functions. This functional concentration forms a risk for survival of the organization. On the other hand, it may have an advantage in terms of efficiency because it avoids dilution of responsibilities that can lead to coordination difficulties.

The last criterion is the **engineering skill of the network**. This criterion measures the capability of the organization to propose a technically viable offer and to deliver the product to its customer. At first sight, the most competitive networks appear to be or have been backed up by national engineering expertise (North Korea and Pakistan). Other networks, like the network that transferred about ten Ukrainian AS-15 airframes to Iran and China in 2000, do not appear to have extensive knowledge about the product, but are capable of efficiently organizing its export to customers.

Based on these criteria, it appears possible to draw up a summary of the vulnerability of our network models. Private organizations are characterized most plausibly by a strong functional concentration, even if they can be very extensive. Based on known examples, it appears that their engineering skills are not uniform, but they are capable of managing the generated flows efficiently. Everything about State networks tends to suggest that they are relatively extensive, but they do not have any noteworthy functional concentration. Their engineering skill depends directly on the competence of the State that they represent.

[86] Anne Platt Barrows, Paul Kucik, William Skimmyhorn & John Straigis, « A System Analysis of the A. Q. Khan Network », Stanford Social Sciences Seminar, December 8, 2005, p. 7.

[87] For the technical part, Khan and possibly some of his close contacts such as Anwar Ali. See Leonard Spector & Haider Nizamani, « New Head of Pakistan Atomic Energy Commission Apparently Tied to 1980s Nuclear Smuggling », *WMD insights*, May 4, 2006.

		Extent	Functional concentration	Engineering skill	Vulnerability
Private or semi-private networks	Centralized networks	Wide	Medium to high	Better	Low because redundancies
	Informal networks	Small	High	poor to good	High
State networks		Wide	Low	Variable	Low

Table 1: Determination of criteria for network models

1.2.2 –Acquisition networks

➧ Functional analysis

Acquisition networks are organized around the objective of obtaining components or know how necessary for national weapons of mass destruction programs, and *a priori* include two elementary functional organizations:

- The first organization, responsible for specification of the need, is used as an intermediary between the product user and the organization responsible for purchasing it. The objective for this part of the network is to define components, systems or technologies that best satisfy the need expressed by the beneficiary. For example in the Iraqi case, the MIC (Military Industrialization Committee) was responsible for this function, based on requests made by managers of production or research centers.
- The organization responsible for purchases/acquisitions must firstly find suppliers capable of satisfying expressed needs, sign direct contracts with these suppliers or with intermediaries responsible for approaching them, and check financial flows necessary to pay suppliers and intermediaries. This organization has many functional similarities with a supplier network, but there are a few differences. In terms of logistics, the network can limit itself to the transport of equipment between front companies set up in other countries and the final user, the remainder of the operations being handled by intermediaries or suppliers. However, this function does not appear to be essential to enable its operation[88]. On the other hand, the financial function is predominant because flows have to be managed within the network itself, including within front companies belonging to it, but also with any intermediaries and with suppliers. Apart from these differences, we can conclude that models developed for supplier networks are applicable to these organizations.

[88] However, the Iraqi case demonstrates that an acquisition network can handle a large proportion of routing.

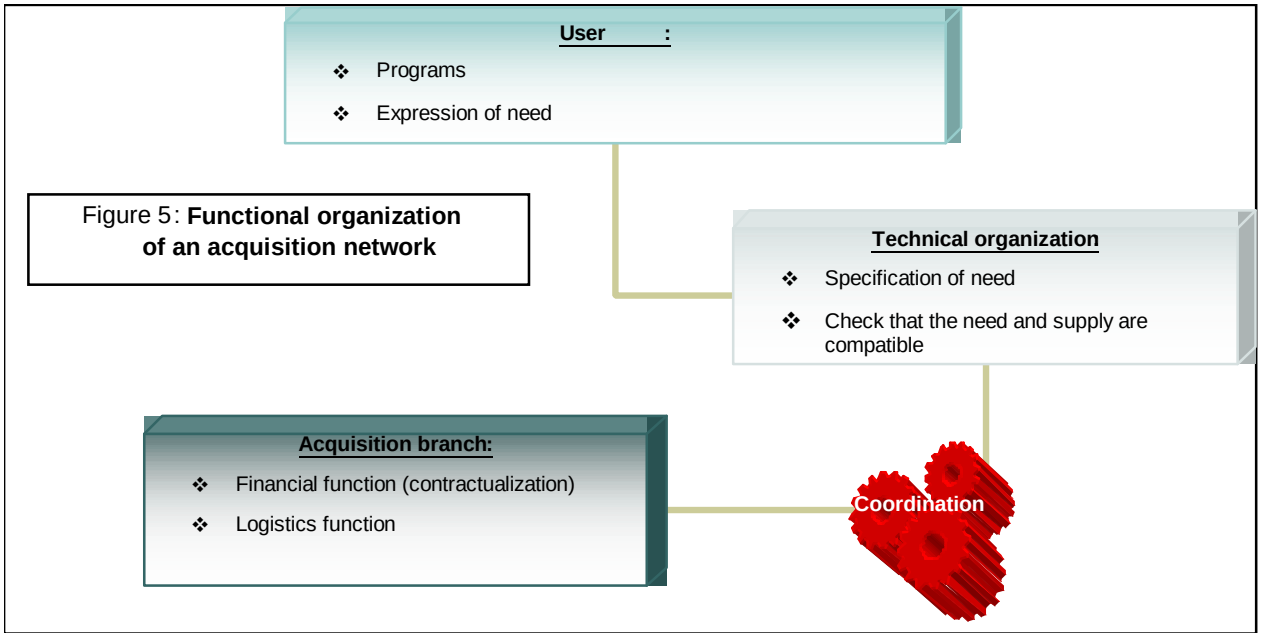


Figure 5: **Functional organization of an acquisition network**

The factor that makes acquisition networks different from other networks is their ability to coordinate these two branches of their activity. As we have seen with the Iraqi example, the coexistence of two concurrent organizations responsible for acquisition, the first dependent on the MIC and the second dependent on the secret services, penalized the efficiency of the network for a long time. These systems were coordinated starting in 1997 enabling the MIC to benefit from unique services offered by the secret services but also to improve the capacity of the secret services to satisfy some needs expressed by engineering centers. This coordination function is not limited to finding the best way of satisfying the need expressed by the user, it must also enable the user to dialog with suppliers indirectly so as to obtain the most suitable product for his need.[89]. This may involve creating a direct contact between the user and the supplier, for example for training or technology transfer purposes.

Since these networks are essentially state owned, the structure of the acquisition branch is centralized like the model presented above. It may be responsible for the coordination function or it may share this responsibility with the engineering branch. Thus, in the Iraqi case, there was a coordination authority between the MIC acquisition branch and the secret services.

In any case, everything suggests that these are long-term organizations with relatively good structures. Even if these networks are considered as being informal in theory and therefore capable of adapting quickly[90], the fact that they are actually based on an environment composed of external players makes them stable in the long term.

[89] For example, this concept of dialog is present in the organization of technical discussions between MIC engineers and suppliers organized by agents working in other countries.
[90] Alexander H. Montgomery, « Ringing in Proliferation », *International Security*, op. cit.

➧ Organization of acquisition networks

Therefore, the vulnerability of acquisition networks depends especially on external players on which they depend for their operation, in other words the front companies-banks-brokers tryptic.

This assembly can be broken down into two main groups:

- Companies belonging to the network, financial institutions or companies that the network sets up in foreign countries to facilitate its acquisition operations. They are remunerated by the acquisition branch and perform direct (but dissimulated) representative functions for the network.
- Companies that do not belong to the network; in general, a series of companies participating in acquisition activities occasionally or involuntarily, such as financial institutions exchanging flows with controlled banks, intermediaries acting on behalf of front companies, or suppliers. There may also be suppliers networks, for example like A. Q. Khan's network or the North Korean network.

In order to facilitate its operation, the acquisition structure may rely on the presence of agents in the field under its direct control; members of secret services (like Iraq) or persons in the engineering branch sent specifically for negotiation of a particular project. Thus, in the Iraqi case, once the first contacts with a supplier or an intermediary had been made, members of the MIC were sometimes sent on site to review the engineering and/or financial clauses of the contract. These agents could also be sent to a supplier to collect a technology or know how, either legally or illegally[91]. They could also provide a courier service for some projects by transporting goods and currencies.

However, their essential role is to act as permanent contact points for companies external to the network, to set up permanent or occasional legal structures (typically front companies) in the target countries so that some projects can be worked on according to needs, and to manage international activities of the network, including financial activities. These purchasers can use two particular methods to improve the security of operations[92]:

- Contact several potential suppliers for a single product; the Iraqi MIC frequently used this method that consists of calling for several bids, sometimes publicly, to satisfy a specific need.[93]. Apart from the economic and technical advantages[94] of such an approach, it is particularly useful to reduce the risk incurred by depending on a single procurement source. In the case of an established program, it is often essential to have access to suppliers capable of selling specific components several times for procurement security reasons, over a fairly long period. For example, production of a given missile may depend on the capability of periodically acquiring critical components that cannot be manufactured in the country. Conversely, in the

[91] For example, this was the case for A. Q. Khan in the 1970s in Europe.

[92] Communication by B. Tertrais to the « Terrorism, Transnational Networks and WMD Proliferation conference: Indications and Warning in an Era of Globalization » conference, July 25-27 2006, Naval Postgraduate School, Monterey.

[93] See also the case of the Indian *Indian Rare Earths Ltd.* company associated with the Delhi enrichment project. David Albright & Susen Baus, « India's Gas Centrifuge Program: Stopping Illicit Procurement and the Leakage of the Technical Centrifuge Know-How », ISIS, March 10, 2006.

[94] Particularly the possibility of obtaining technical data on the equipment and thus refining the definition of the need, or even obtaining modifications on components.

case of a single operation, this method can minimize losses if the authorities in the country concerned discover the matter.

- ➡ Dissimulate a critical component in a list of commonplace goods; this technique may have two end purposes. Legitimize a call for bids to a supplier originating from a company in a given business by dissimulating a product required by the network among elements that could effectively be useful for this company's activities[95]. Make the task of national control authorities more difficult by increasing the volume of requests that have to be treated by them.

The increased number of participants also appears to form a complicating trend in terms of organization of acquisition networks. Thus, a first intermediation company replying to a particular call for bids from a front company could itself call upon several other brokers that may be located in different countries. These intermediaries contribute to increasing the number of logistic and bank operations related to the acquisition and transport of a given product, making identification of the final destination and detection of a given operation more difficult. This is particularly the case when, as we have seen above, these intermediaries usually disguise the nature of the final user or even the identity of the addressee, when they know it.

The inherent nature of intermediation companies is an additional advantage influencing the effectiveness of operations in an acquisition network. They are composed essentially of individuals relying on simple commercial structures[96] and that are very mobile (financially and geographically) so that they can operate from any country. Consequently, they can partly overcome controls imposed on them by setting up in a State that does not have any legislation governing their activities. For example, consider a broker operating from Switzerland to manage transactions between a European company and a front company set up in Hong Kong, without taking any legal risk[97]. However, this geographic mobility is largely theoretical. In order to operate, brokers rely on companies set up in a given country, with which they have specific contacts[98]. The intermediaries themselves are no doubt extremely flexible, but the working environment on which they depend is not.

Financially, acquisition organizations use a network of companies that enables them to conceal the origin of the funds used and consequently the end purpose of operations. Some of these institutions are more or less directly under their control. Apart from the use of cash payments so as to escape the vigilance of financial monitoring services, the use of transfers in preference to letters of credit is also becoming more frequent[99]. Opening of a letter of credit requires deposition of documents, particularly the contract between the seller and the buyer, which when completed enables payment to the seller. Therefore, the letter of credit leaves a trace that can be detected by financial monitoring services and that can be used to determine the exchanged goods or services. On the other hand, a bank transfer is not linked to any documentation whatsoever and is consequently more difficult to use even if it is detected. This method is probably used to

[95] David Albright & Susen Baus, « India's Gas Centrifuge Program: Stopping Illicit Procurement and the Leakage of the Technical Centrifuge Know-How », op. cit.
[96] A few employees and sometimes only a postal address. It is not unusual that brokers create mushroom companies to carry out some specific operations.
[97] http://www.nisat.org/publications/armsfixers/Chapter1.html
[98] This is the case particularly for the transport of goods or even financial operations
[99] Author's Interviews, June 2006.

finance operations within the network (for example activities of front companies), and also with external players.

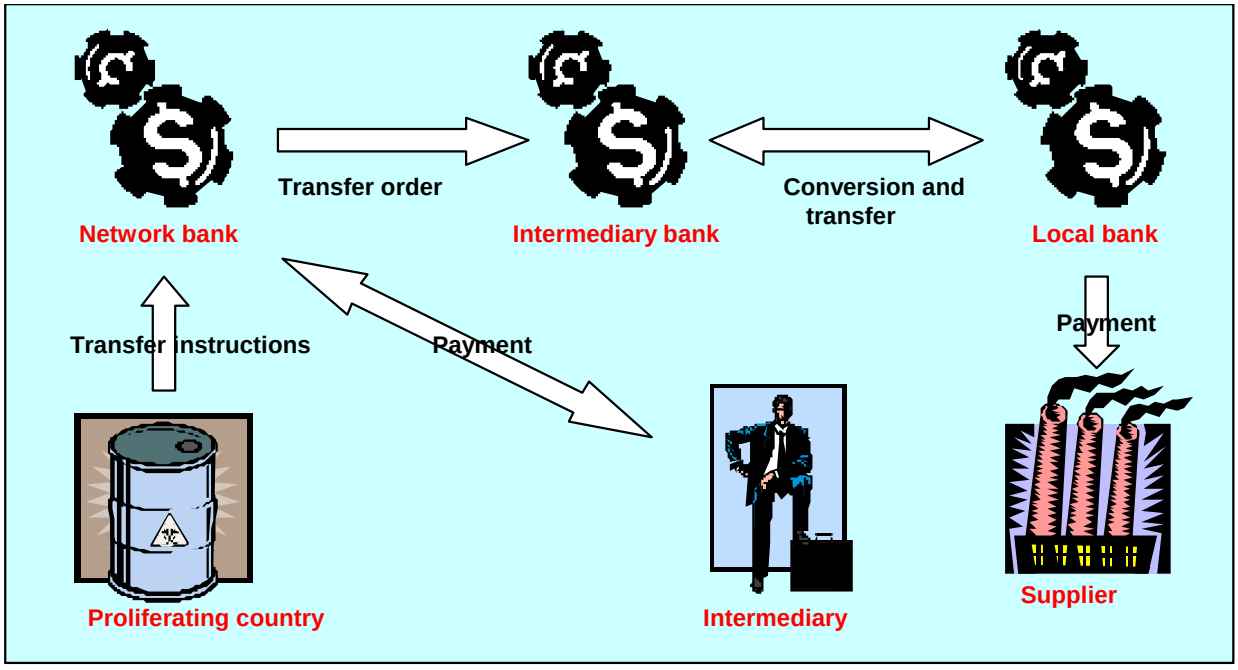


Figure 6 : Operating scheme for a bank transfer associated with acquisition of a proliferating good

Despite the diversification of financial intermediaries, proliferation networks apparently continue to rely on only a handful of banks that act as genuine nerve centers for their confidential activities. For example, the Syrian central bank was one of the necessary passage points for financing of the Iraqi acquisition network but also for profits obtained through the illegal sale of oil products to bypass the "oil for food" system[100]. Similarly, the *Banco Delta Asia* was probably used as Kim Jong Il's financial reserve[101] (supplied firstly by various traffic and by generous donators) and also to financially maintain Pyongyang's acquisition network. By freezing North Korean credits managed by this bank, the American Treasury department created a genuine chain reaction on financial institutions further downstream[102]. However, everything suggests that networks are capable of reorganizing their financial structure if one of their centers is neutralized, relying on trusted institutions. Thus, it appears that Pyongyang has already initiated such a procedure to replace the *Banco Delta Asia* with a Singapore entity[103]. The North Korean regime also seems to be attempting to open accounts in Russian or Vietnamese banks under the names of individuals rather than companies[104].

[100] Report by the Iraq Survey Group (ISA).
[101] « U.S. now Believes Macau Bank Account was Kim Jong Il's « personal » slush fund », *East-Asia Intel*, July 26, 2006.
[102] Thus, the Chinese Central Bank would also have frozen North Korean credits, like several European banks. Ibid.
[103] « North Korean counterfeiters back in business, via Singapore bank », *East-Asia Intel*, August 9, 2006.
[104] « North Korea opens bank accounts in Russia to avoid scrutiny of leadership cash flow », *East-Asia Intel*, September 6, 2006.

➧ Vulnerabilities of a suppliers network

While defining vulnerability criteria for suppliers networks, we have defined a set of parameters that also appear applicable to acquisition organizations.

However, the special feature of these networks is that due to their institutional nature[105], and therefore their size and their functional deconcentration, they are more vulnerable technically than structurally. The main difficulties are the ability of the States to precisely define their need, to find suppliers capable of responding to it satisfactorily, and to efficiently organize the interface between the acquisition branch and the end user. Therefore, the level of progress of the weapons program plays an essential role in determining the efficiency of the network.

Thus, a player without any engineering or technological experience who needs to acquire off-the-shelf capacities or who would like to build up his own competence, should make use of networks of suppliers capable of proposing a complete offer. For example for missiles, such a State could turn towards North Korea, China or Russia. In this case the acquisition system could be relatively simple compared with the model described above, since most operations are handled by the supplier. Therefore, its vulnerability is related more specifically to the national capability of understanding and controlling the technologies supplied (including maintenance of systems and their operational use in the case of missiles) than to its organization. In financial terms, the network may be limited to direct payment of the supplier in the most discrete form (cash or by bank transfer) or even to opening of letters of credit giving priority to contacts between its own bank institutions and bank institutions in the supplier's network. Similarly, if it can make use of brokers or intermediaries, direct contact with these brokers or intermediaries can considerably reduce its visibility towards the outside and risks of temporary neutralization of its activity. Libya is the case that most closely corresponds to this model among known acquisition networks; for example Libyan services made direct contacts with A. Q. Khan for the acquisition of an enrichment capacity, payment being made at least partly in cash.

For States with national programs, acquisition of some key components requires the assistance of supplier States that are not proliferation countries[106]. In this context, it is essential to set up an international network of companies and persons acting on behalf of the acquisition activity, in accordance with the developed model. As a result, this part of the network forms a possible target for national or international organizations made responsible for struggling against proliferation. However, the level of engineering skills in the proliferation country will be controlling in determining the efficiency of the acquisition function. Thus, a distinction can be created between States with a simple systemic capacity (the possibility of producing a system from these main components) and States capable of manufacturing key components of the system[107]:

- States that simply have a systemic capacity must acquire some complete specific components for which acquisition attempts can be more easily detected. If they can

[105] Ignoring private acquisition organizations such as sects and terrorist movements, for which the scale of the means set aside and the completely illegal nature of their activity are beyond the scope of this study.
[106] Which are qualified as Source States in the remainder of the study.
[107] Such an elementary distinction is described in detail for the nuclear field in an article by William C. Potter, « The diffusion of Nuclear Weapons », in « The Diffusion of Military Technology and Ideas », Stanford University Press, 2003, pp. 169-170.

turn towards other networks to access them (the suppliers bring in their own engineering capability), these states are sometimes obliged to call upon external suppliers. This situation creates a two-fold vulnerability for the acquisition system:

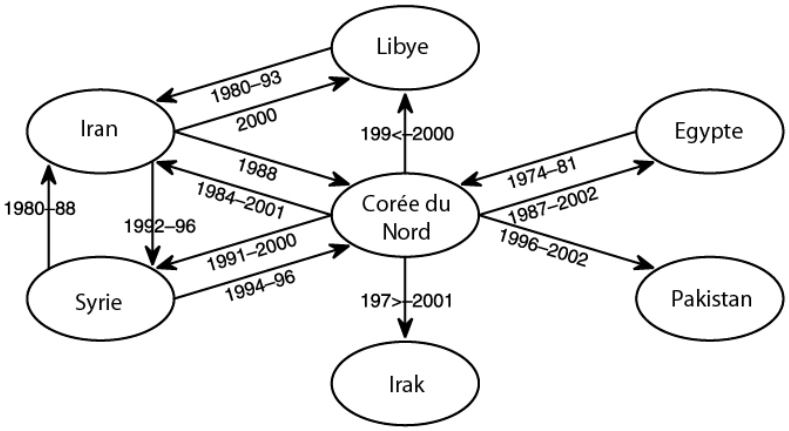
- ⇨ Coordination between the engineering branch and the purchasing service becomes essential. For example, a failure in this field can result in the acquisition of a product that is too different from the user's specifications for it to be useful[108].
- ⇨ Dependence on a restricted number of suppliers; in the domains considered (nuclear and missiles), there are not many companies with the required know how to produce complete subsystems[109]. Furthermore, the goods considered are relatively tightly controlled by the national authorities since they are mostly technologies related to the military field.

➡ States capable of producing key components for the system may rely on the acquisition of elementary dual-use goods, which are less visible to control services when purchased. This degree of technical control considerably reduces the risk of detection of the network's activities.

After considering these elements, it appears that the interaction between the supplier networks and acquisition networks plays a special role in terms of proliferation. As we have seen elsewhere in the case studies mentioned above, several relations have been woven between networks since the beginning of the 1990s that tend to indicate the development of a form of globalization of proliferation exchanges.

1.2.3 – Interactions between networks: towards globalization of proliferation

Liens entre réseaux de prolifération de missiles balistiques réseaux de 2e génération et niveau, 1974-2002
d'après Alexander Montgomery,
Ringing In Proliferation: How to Dismantle an Atomic Bomb Network



SOURCES: Missile proliferation data are from the Nuclear Threat Initiative, *Country Profiles,* and extend through 2002. Individual and minor incidents were discarded.
NOTE: Only the core second-tier proliferators appear in this figure; other countries that received only limited assistance (e.g., Sudan and Yemen) are excluded. Uncertain dates are marked as < (beginning of decade) or > (end of decade). Minor nodes are excluded; nodes are placed for clarity.

In the examples mentioned above, the organizations involved have carried out two types of operations, either with companies located in non-proliferation States, or with other proliferation networks.

In the latter case, movements of part of material, immaterial and financial flows may appear uncontrollable to the extent that flows do not involve the recourse to legally established companies.

[108] Note the 1995 example in which IISs acquired inertial control units for submarine-launched missiles, which proved to be unusable by the engineering centers working on the missile program.
[109] For example, there are only two companies in Europe that make navigation systems (complete and usable for ballistic missiles): Thales and SAGEM.

However, the very nature of the proliferation networks is such that exchanges between them are impossible without recourse to external companies. This is due particularly to the fact that known suppliers are incapable of offering an entirely indigenous product. For example, after the Khan network detached itself from the acquisition organization of the Pakistan nuclear program, it had to turn towards foreign suppliers for some components. Therefore, unlike the theoretical models described herein, proliferation networks cannot operate without some interaction with non-proliferation entities, since they perform both acquisition and sales activities.

Nevertheless, the creation of networks weaving links between proliferation organizations is a worrying development since it tends to strengthen resistance of each organization to external disturbances. In the ballistic missiles field, it is particularly striking to observe that cooperations that were created between networks in the 1980s and 1990s tend to put North Korea in a position which is no longer central, thus facilitating mutual cooperation between its former customers. The result today, having started from a star structure organized around the North Korean network, is a more dynamic decentralized structure that is also more difficult to neutralize[110]. Other entities, for example such as China or Russia, are also attached more peripherally to this network of networks.

For nuclear proliferation, it is clear that the structure of relations between networks remains centralized, with the core being the Pakistani network. However, the development of nuclear capacities in Iran and North Korea could eventually lead to decentralization like the model for the ballistic case. One of the specific features of the nuclear network is due to the fact that the central organization holds and proposes knowledge and know how necessary for the others. In conclusion, the structure of organization networks largely corresponds to the level at which know how (technologies, knowledge, experience[111]) is distributed between the various entities involved. Eventually, this global nuclear network could become decentralized due to the emergence of new players capable of distributing or exchanging their knowledge and know how among themselves without passing through the center.

[110] Alexander H. Montgomery, « Ringing in Proliferation », op. cit., p. 172.

[111] Experience is what can only be learnt from tests, failures and trial and error operations for a specific program. As demonstrated by William Potter (and to a lesser extent by Alexander Montgomery), diffusion of technologies between countries takes place not only by the transmission of data or components, but receivers also have to be able to understand and control them. This is a phenomenon influenced by political, historical, engineering and economic factors that depend on the countries concerned. W. Potter, « The diffusion of Nuclear Weapons », op. cit.

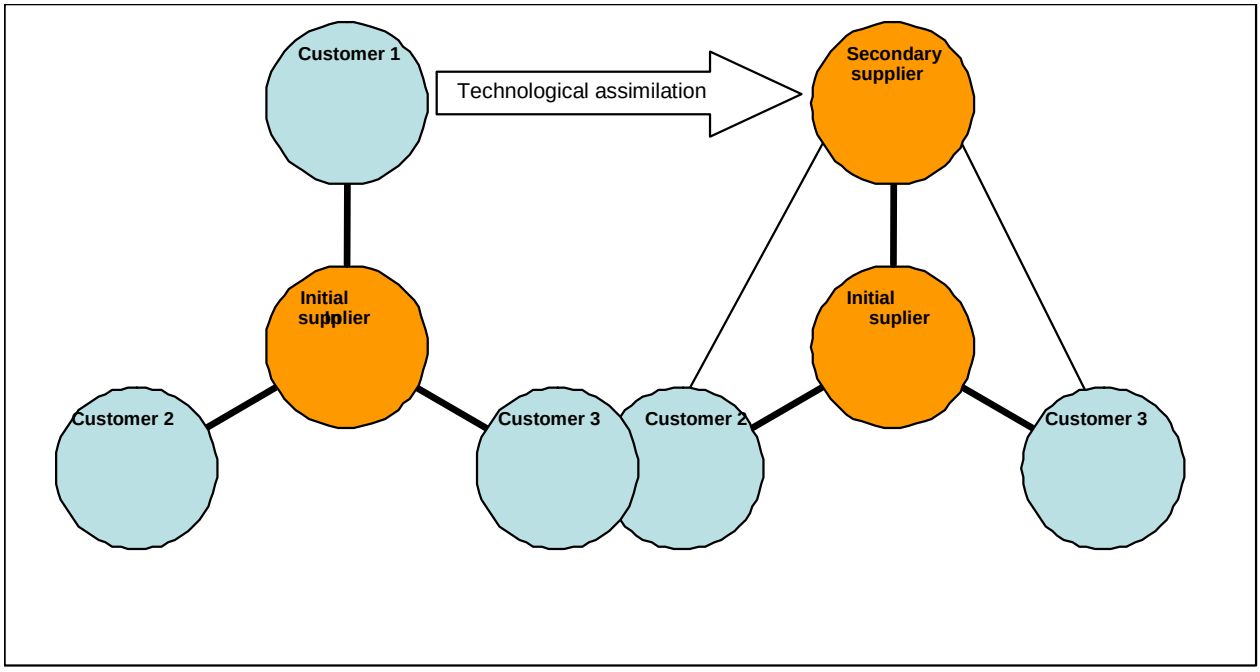


Figure 7: Development of a Network under the influence of understanding and control of Technologies

It is worthwhile to note that apart from technical interaction between networks, other links have also tended to develop within the small world of proliferation. Firstly, they relate to network's agents within the source States[112], in other words intermediaries, brokers and other hired hands that networks use to perform some of their operations. Even if most organizations use their own agents to carry out operations in other countries, it is not unusual for them to call upon these intermediaries. Thus, it appears that the Indian nuclear acquisition network relied on South African entities that also worked for the Khan network[113]. The networks may also decide to federate their acquisition efforts in source States within the framework of a common program. The program for development of the Argentine–Egypt–Iraq Condor-2 missile in the 1980s was managed by a transnational company the CONSEN group, responsible for financial and engineering supervision aspects of the program and for acquisition activities in other countries. This company had called upon intermediaries, particularly including Abdel Kader Helmy, whose role was to purchase some necessary components for the program, in the United States[114]. Setting up of the Russian-Iraqi ARMOS *joint venture* as part of the acquisition efforts made by the Iraqi network uses a similar logic[115].

Considering the increase in cross cooperation between proliferation countries, pooling of some acquisition operations appears to be unavoidable. It could be in the form of isolated mutualization of logistic and financial means so as to improve the efficiency of managing material and immaterial flows between the networks concerned. The use of the

[112] This is the term used to refer to States in which companies whose proliferation networks are attempting to acquire goods or technologies are located. By extension, it also includes tax havens, States flying convenience flags and countries acting as turntables for traffic.
[113] David Albright & Susen Baus, « India's Gas Centrifuge Program: Stopping Illicit Procurement and the Leakage of the Technical Centrifuge Know-How », op. cit.
[114] His arrest in 1988 was largely the reason why Egypt abandoned the program. http://nti.org/e_research/profiles/Egypt/Missile/index.html
[115] See § 1.1.2.1.

transport means of one network for an operation carried out by another network is not impossible[116], reflecting the use of bank institutions operating for one network on behalf of another[117]. But if these operational reconciliations can increase, they will be limited due to vulnerabilities that they induce on national systems. The various players in the market need to assure that complete or partial neutralization of a friendly network does not cause neutralization of its own organization. Furthermore, as emphasized by Alexander Montgomery, even if networks are tending to move closer to each other due to the similarity of their structure and the contacts that they can maintain with a common supplier, the existence of competition between them or even bad political relations reduces the risk of them cooperating directly[118].

In this case, relations that can be made between networks and the outside world should continue to be an element controlling their existence and their operation.

1.2.4 –Interactions with the outside world and adaptation capability of networks

Apart from interactions that they develop among themselves, proliferation networks maintain close relations with other players. This includes commercial and functional (for example logistic), and even political relations. As we have already seen, proliferation networks do not operate in a closed loop; their technical dependence on source States, the need to move their capital to perform their operations, management of material flows or neutralization attempts have a direct influence on their operations.

There are two types of external players in the activities of a network:

- Friendly players: apart from customers, some countries, institutions, players, act for the benefit of networks for political or economic reasons. For example, the Iraqi network benefited from the support of some of its neighboring countries to set up bank accounts designed to manage its bank transactions. This category also includes intermediaries not acting under the direct and exclusive control of the network.
- Hostile players: networks are confronted with actions that could reduce their efficiency or undermine their operations, from groups of suppliers or States attempting to neutralize them. For example, the United States plays a key role in the fight against networks, particularly in launching the *Proliferation Security Initiative* and through their efforts to dismantle financial operations. Similarly, efforts made by intelligence services in Western countries to dismantle organizations carrying out traffic endanger the very existence of proliferation networks. The possibility of seeing their operations exposed by intelligence actions (including infiltration) is not non-existent. Thus, Urs Tinner, who worked in Malaysia for the benefit of A. Q. Khan as part of the Libyan contract, could have acted on behalf of the CIA[119] and supplied the American agency with information about the network's activities. In any case, in theory this situation makes it necessary for proliferation

[116] For example, some networks make use of a large merchant fleet that they can make available for their customers or suppliers to escape from interception within the context of the PSI. See B. Gruselle, « Cruise missiles and anti-access strategies», FRS Study report, December 2005, p. 48.
[117] Thus, a Chinese Airline company, Great Wall Airlines, linked to the Chinese Great Wall Industries Company, was sanctioned by the American Treasury department for being used to freight components to Iran and North Korea « U.S. sanctions Chinese airliner for freighting WMD to Iran, N. Korea », *East-Asia Intel*, September 6 2006.
[118] Alexander H. Montgomery, « Ringing in Proliferation », op. cit., p. 177.
[119] « The Double Game in the Nuclear Poker », *Focus*, March 15, 2005.

organizations to be reactive and dynamic, in other words capable firstly of protecting their operations so that they cannot be exposed, and secondly of reorganizing them so that they can continue to function if their environment is disturbed. It has been found that known networks are not always capable of adapting when faced with various difficulties. More precisely, it appears reasonable to put the difficulties into three categories to analyze them:

- ⇨ Technical difficulties: changes to export control systems tend to broaden the field of controlled components and technologies (although not all countries have exactly the same standards). In fact, this has already forced networks to concentrate their acquisitions on more and more elementary components to escape the vigilance of organizations responsible for control. But their technical competence effectively limits their capability to adapt to the broadened spectrum of controlled components. Thus, if this trend continues, they will need to carry out some of their acquisitions more and more illegally, increasing risks for their agents and intermediaries[120].
- ⇨ Logistic problems: setting up organizations to transport goods acquired in foreign countries is usually based on the use of transport or freight companies that do not belong to the network[121]. If the source State belongs to a proliferation network and the means used belong to it, the risk of disturbance is small[122]. On the other hand, if goods are transported by a private company on a ship or commercial cargo aircraft not belonging to a proliferation state, several events can expose the operation and functioning of the buyer network, for example interception of the cargo on the open sea or above the national air space of a hostile player. However, this type of disturbance does not appear to be sustainable in that *a priori* it only exposes the front company to which the goods are addressed. Therefore the network concerned can react quickly by using other front companies under its control (or possibly creating others). Moreover, the lack of any external controls or code of good conduct for logistics businesses (transport and freight) and the economically profitable nature of this economic activity, makes the companies concerned fairly lax when examining the identity or nature of their customer[123]. Endangering or durably neutralizing intermediaries set up in foreign countries appears to be more harmful for a network (or a network of networks). Even if they can be replaced, brokers play a central role in the functioning of networks as we have seen above, and their neutralization can damage the functioning of these networks in the long term. However, to achieve this, the States must be in a position to pursue and arrest the intermediaries involved.
- ⇨ Bank difficulties: functioning of proliferation networks depends on the possibility of these networks to transfer funds among themselves, and between themselves and their agents and their customers and suppliers. Some of these transactions take place within the international banking system and as we have seen, proliferation

[120] However, to reach this situation, organizations responsible for control must be capable of efficiently monitoring an increasing number and a broader variety of goods and technologies. It also requires international harmonization of criteria used by inspection systems and their effectiveness (see below and chapter 2).
[121] Author's Interviews, November 2006.
[122] For example, this is the case in North Korea. This case also includes the use of diplomatic communication channels
[123] Author's Interviews, November 2006.

organizations call upon private or public bank institutions to perform these operations. Thus, some of the Iraqi funds intended to supply the acquisition network passed into individual accounts opened in Syrian, Lebanese and European banks. Freezing credits deposited in these "trusted" banks can profoundly disturb the operation of networks because, apart from associated financial losses[124], in practice it prevents remuneration of intermediaries and suppliers, who only remain motivated to participate for financial reasons. Furthermore, it can create cascade effects on States in which downstream side financial institutions are located and which also perform similar actions to avoid being sanctioned[125]. The difficulty that the network will have in recovering is more or less severe depending on the level of the financial institution concerned (see figure 8). Thus, neutralization of local banks that only manage an infinitely small part of network resources does not create insurmountable problems because it can be assumed that financial flows can pass through other institutions at the same level. On the other hand, neutralization of intermediary banks is a bigger problem because they manage larger amounts and they also control flows to a series of other local players. Furthermore, unlike institutions under the more or less direct control of the network, it appears possible to neutralize them because they usually are commercial companies sensitive to the threat of commercial sanctions, or they are under the jurisdiction of governments on which political pressures can be applied[126]. Replacing compromised intermediary institutions can cause serious difficulties for proliferation networks; much of the network has to be reconstructed, but a trusted bank capable of managing transactions with local banks also has to be found. For example, these difficulties can be seen clearly in management of North Korean credits deposited in the *Banco Delta Asia*. Pyongyang appears to be having a great deal of difficulty in finding a company that will take the risk of handling this type of activity on its behalf.

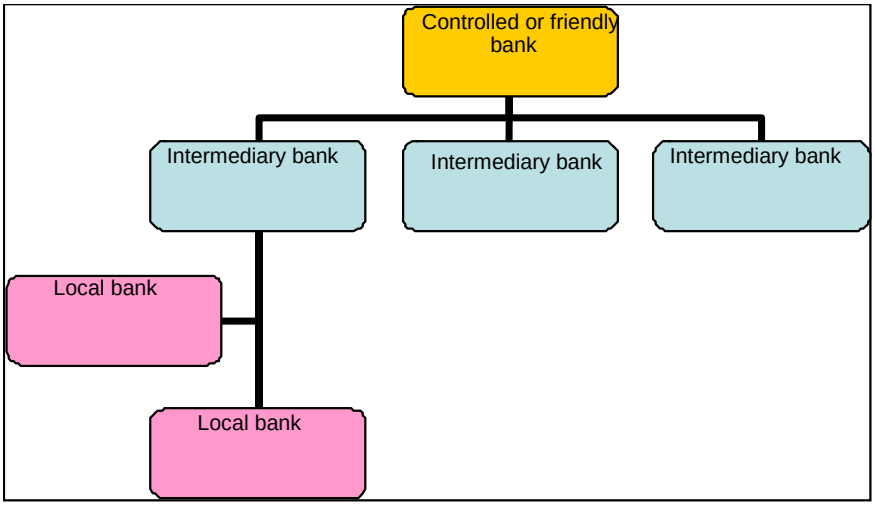


Figure 8: Sensitivity level of financial institutions working for the benefit of a network

[124] These losses can be very high if this freezing affects banks at the heart of financial activities. See above.
[125] Author's Interviews, November 2006.
[126] Thus, the fact that the Chinese Central Bank decides to make an investigation on North Korean credits deposited in China illustrates the sensitivity of these relay institutions to economic pressures.

The influence of developments in world trade on proliferation networks is also one of the questions being raised about how this phenomenon is changing and its interaction with external players. Although globalization and dematerialization of exchanges are not the causes of networks appearing, they have contributed to development of their operation[127].

Firstly because technologies have become more accessible due to the expansion of information technologies. Thus, a suppliers organization can now transfer this information to its customer quickly and confidentially and an acquisition network can even obtain engineering support discretely. The benefits acquired by networks due to the dematerialization of financial exchanges are not so evident. Firstly, this dematerialization means that sums of money can be moved between financial institutions, agents and suppliers or customers quickly and efficiently. However, the discretion of these exchanges is questionable because intelligence services can monitor computer exchanges more easily and process them more efficiently than for paper exchanges. However, traffic is more difficult to detect based on computer exchanges if there is no documentation base associated with the transaction[128].

The increase in the volume of exchanges also makes it easier to dissimulate traffic within legitimate transactions[129]. For sea shipping alone, the quantity of goods transported by sea increased from 2 500 to 5 800 million tonnes between 1970 and 2005[130], this growth being concentrated particularly in the Asia-Pacific zone. In particular, transport by container carriers has grown strongly, firstly due to the increase in the carrying capacity of ships, but also due to the modularity of this type of transport[131]. Development of this transport mode has several advantages for proliferation networks:

- The number of large operators in the sector (charter companies, transporters, handlers) has increased and at the moment they do not have the physical means to assure traceability of loadings. Therefore, a proliferation company can conceal a sensitive component in a container and thus limit the possibility of it being detected.
- Transshipments are a means of taking advantage of the more or less lax nature of control over goods in transit in the main commercial hubs. For example, it may be advantageous to choose to have merchandise delivered in Dubai or Taiwan rather than Marseilles or Singapore, where controls are stricter.

The expansion of worldwide exchanges has largely contributed to the distribution of technologies to a larger number of industrial players. Therefore, proliferation networks can now call upon companies with required know how or products and located in States in which control systems are less efficient than elsewhere. The Khan network's use of the Malaysian company, SCOMI, is an example based on this logic. The international distribution of technologies contributes to limiting the extent to which proliferation networks are affected by some States extending the lists of goods controlled for export.

[127] J. Caves, « Globalization and WMD Proliferation Networks: The Policy Landscapes », *Strategic Insights*, Vol. V, Issue 6, July 2006.
[128] See § 1.2.2 in this document.
[129] According to the World Bank, the growth in world trade was 8.9% in 2005, and 11.8% in 2004.
[130] http://www.ac-rennes.fr/pedagogie/hist_geo/ResPeda/mondialisation/commerce/cemaritimegraphes.htm
[131] A. Frémont, "Containerized shipping networks: spinal cord of globalization", *INRETS*, October 2005, p. 4.

Finally, globalization provides an opportunity for existing proliferation networks firstly to improve their functioning, and also gives them tools to protect themselves from attempts made by States to neutralize them. However in order to use these tools, systems must have technical capabilities and an adapted functional organization. For example, a new proliferation player cannot take advantage of the distribution of technologies if he does not have sufficient knowledge, since he would be incapable of developing and producing a complete system starting from elementary components. To do this, he would have to call upon a supplier with the necessary abilities, like Libya called upon the Khan network to acquire an off-the-shelf enrichment capacity.

1.3 – Prospects for development of illegal acquisition networks

Everything suggests that proliferation of technologies, goods and know how related to weapons of mass destruction and their vectors operates more or less like a market. The existence of a demand produces creation of a supply, the supply being more or less complete in engineering and logistic terms.

But the match between the needs of buyers and the capabilities of the market to respond to them is by no means assured. Despite the efficiency of its organization and ceaseless efforts, the Iraqi acquisition network was incapable of completely satisfying the needs expressed by the regime. The pressure created by the United Nations inspection and control regime obviously contributed to this failure. By obliging the Iraqi system to operate using clearly illegal and the most discrete possible means, they probably prevented it from getting into contact with suppliers capable of efficiently satisfying the need. Thus, it is probable that the breakdown of negotiations between Baghdad and the Khan network was due to fears of the Iraqi secret services that the matter would be discovered.

However, the appearance of supplier networks capable of offering a complete and technically reliable product will tend to make the market more efficient and consequently increase the risks of proliferation. The case of privatization of A. Q. Khan network appears to be particularly worrisome, in that this was the first time (in the nuclear field) that an organization operating on an essentially commercial basis was in a position to offer a complete capacity beyond the control of the national authorities. Other organizations of this type could exist now or in the future. This is already the case for missiles with the North Korean network that could extend its activities to include the supply of nuclear capacities. But the State-controlled nature of this network partly limits the nuisance.

Another worrying trend is developing with the possible entry of non-state purchasers such as terrorist groups onto the market. Efforts made by the Aum Shirnikyo sect to acquire several tonnes of chemical precursors in order to make weapons prefigure such a development[132]. Considering the nature of the terrorist activity at the beginning of the XXIst century, micro-proliferation of weapons of mass destruction could emerge, being supplied by suppliers-assemblers[133] that are also non-state suppliers, or rather are independent from States, like the Khan model.

[132] Scott Jones, « Black Market, Loopholes and Trade Controls: The Mechanics of Proliferation », 2005 Carnegie International Non-Proliferation Conference, November 8, 2005.
[133] In other words capable of providing a complete system offer.

Finally, although it is important to apply pressure on the demand (particularly through non-proliferation actions), we also need to accelerate the development of an effective response controlling how the supply changes. The objective is not to attempt to systematically neutralize suppliers offering elementary components, even if this were desirable, but rather to prevent the appearance and development of private networks capable of delivering a complete system to any customer, and ready to do so. These organizations present the greatest threat in terms of non-proliferation.

2 – What means and policies should be adopted to neutralize proliferation networks?

Simply strengthening existing non-proliferation tools does not seem to provide a response to the development of proliferation network activities. The objectives are firstly to reduce demand, and secondly to neutralize traffickers of goods and technologies that supply the demand. Furthermore, both the demand and the supply are likely to become more complex and extend to include private players on which the non-proliferation policy has little influence.

In general, the effectiveness of the struggle against proliferation networks should be based on three basic points:

- **Mapping of network activities**. Characterizing the structure of a given network provides a means of determining which are the essential players, their roles within the organization and thus selecting the best targets for actions aimed at neutralizing the network in the long term.
- **Long-term neutralization** of key functions of networks; by terminating specific logistic, financial or technical activities within a network or by neutralizing key players in its operation (intermediary companies or banks, coordinator, etc.).
- **Interruption of essential flows,** including material, immaterial and financial transfers, can durably degrade operation of networks.

Therefore, setting up a proliferation network neutralization policy should be based on reinforcement of a set of tools that operate in a complementary manner. Firstly, it must relate to the existence of a detection function, the role of which is not only to identify suspicious flows, but also to expose organization of the network and its key players. Based on this capability, two types of measures can be used:

- **Repression** is aimed at neutralizing the activity of network agents or preventing the end of operations undertaken by them. For example, the objective may be to prohibit access of the network to intermediary or relay banks, or *a priori* to prevent export of goods or technology transfers organized for the benefit of the network or one of its customers.
- **Interception** consists of blocking transfers or operations in progress. This can be done within a legal framework (customs seizure, freezing accounts, sanctions) or a military framework (interception of cargo at sea).

The objective in this part is to determine how these tools can operate considering previously studied network models. In particular, adaptation of detection, repression and banning means to the development of proliferation traffic should be evaluated in order to suggest possible options for improving their efficiency.

Another major challenge is the coordination of national and international approaches in terms of the struggle against networks. The use of international trade mechanisms enables networks to partly escape from reinforcement of means used by States. This is why it is essential to develop international tools to fight against proliferation networks, and this could be done based on existing means. But approaches that should be undertaken to make the various economic players take this question into account more accurately in their daily management need to be considered. Particularly because the

privatization phenomenon of proliferation activities should result in economic players being more involved in the operation of the networks.

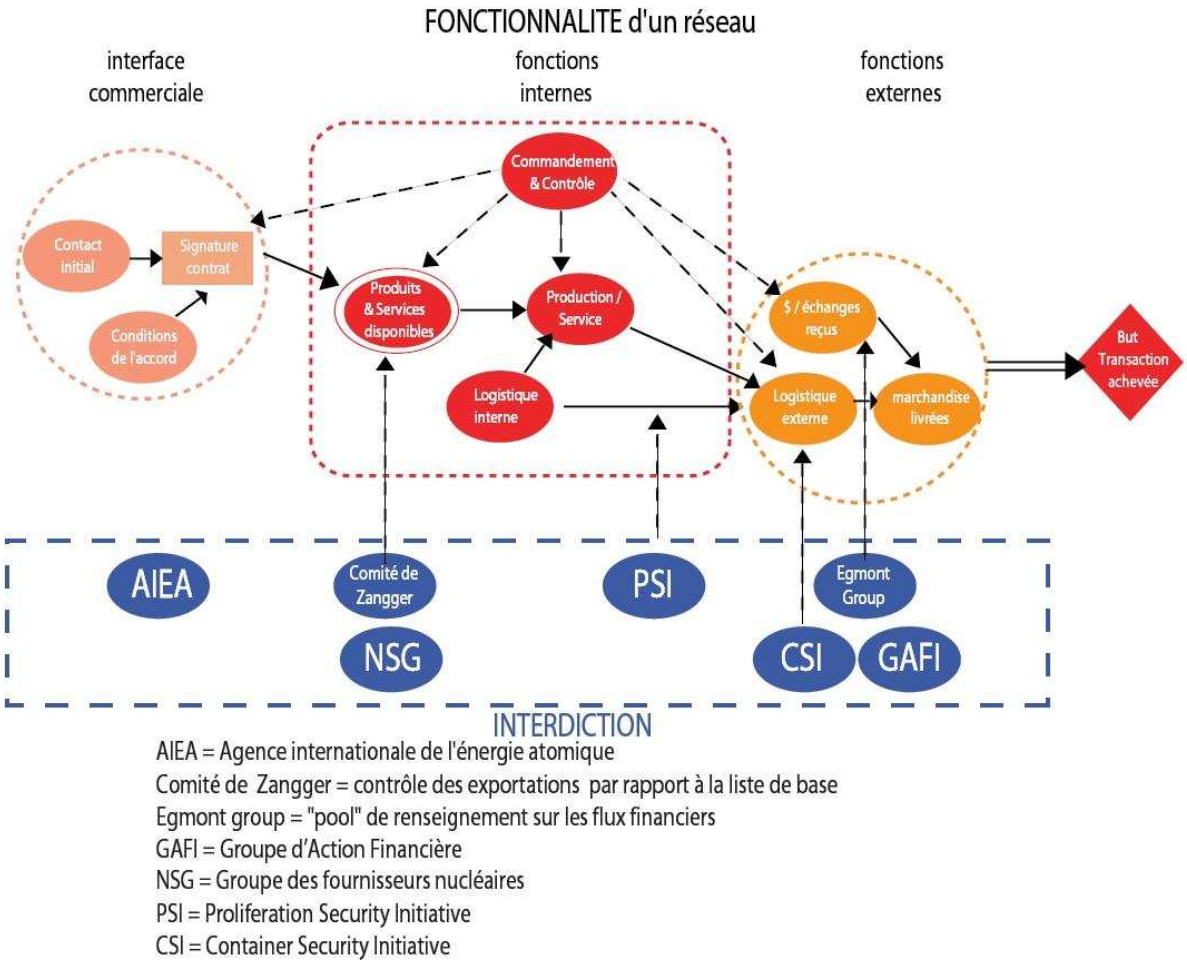


Figure 9: Theoretical organisation of the struggle against proliferation traffic

2.1 – Intelligence faced with proliferation networks

The efficiency of a system designed to neutralize proliferation network activities is largely based on the ability of intelligence firstly to detect operations performed by these networks, but also the possibility of specifying their structure and operating method.

The work consisting of "mapping" networks is based firstly on surveillance of flows, people and companies in order to detect proliferation activities. Starting from this point, the objective should be to tie these pieces together to form a consistent set. For example, surveillance of one identified intermediary of the Khan network must make it possible to identify supplier companies, intermediary banks and possibly other agents belonging to the network. Apparently, two pitfalls need to be avoided in this procedure. Firstly, there can be a strong temptation to block an operation in the network before fully characterizing the network, at the risk of seeing it reorganize and therefore the players who had been surveyed having disappeared although their surveillance could have helped identify a key node[134]. On the contrary, not acting until the network has been fully characterized can allow transactions to be completed with dramatic consequences in terms of dissemination of nuclear or missile technologies. For example, if action is taken too late, a network might obtain key technologies for building up a national program. Efforts in the subject depend on the capability of intelligence services to obtain complete, precise and sufficiently reliable information to identify the role of each player and the end purpose of the transactions. There is no doubt that such a task is physically impossible, considering the potential complexity of the networks, and particularly diversity in terms of the extent and spectrum of their activities, functional concentration or even dissimulation efforts that are undertaken. Therefore, a compromise has to be found between the need to produce the most detailed and complete possible mapping and necessary actions either against a specific transaction, or against a player considered to be sufficiently important so that his neutralization would affect network activities in the long term[135].

2.1.1 – Organization of intelligence for detection and investigation of proliferation networks

A variety of competence in intelligence to handle engineering, financial, logistic and human aspects of operation of proliferation networks must be created to match the complexity of these organizations.

Furthermore, from an engineering point of view, intelligence services are faced with the complexity and variety of the domains treated. As we have seen, networks concentrate on acquisition of elementary goods to escape from control systems that must therefore have high technical skills to understand the end use of these goods. Thus, in the field of proliferation more than in the other fields (terrorism, drug traffic and weapons traffic),

[134] Notes from the « Terrorism Financing and State Responses in Comparative Perspective », Center for Contemporary Conflict conference, November 4-5, 2005, are particularly interesting on this question.
[135] The case of dismantling of the Khan network is based on this compromise logic, American intelligence services probably having postponed action against the network so as to be able to strike as close as possible to the heart of the network. Auhor's Interviews, November 2006.

intelligence must be capable of relying on its own or external resources in order to deal with the engineering aspects.

In terms of organization of national intelligence, the three large Western countries (the United States, United Kingdom and France) have *a priori* similar tools. Each of them has an internal security service and one or several organizations dedicated to external intelligence. Each of these organizations is capable of monitoring activities performed by networks on its own country, and their ramifications outside the country. In the field of proliferation, they have generally developed their own skills by bringing together intelligence experts, technical specialists and persons familiar with regional questions. These skills may be supplemented by bringing in engineering services of Ministries of Defense.

Thus, France has a number of organizations within the Homeland Surveillance Directorate (DST), the General Directorate of External Security (DGSE) and Military Intelligence Directorate, responsible for proliferation questions and that also benefit from the support of the General Delegation for Armament (DGA). The National Directorate of Research and customs investigations that reports to the Ministry of Finance is complementary to this system. Its investigation capacity is reinforced by the possibility of customs agents accessing commercial documents of companies, such that it can make a link between engineering and financial problems surrounding proliferation questions[136]. Thus, Customs investigation units could usefully participate in tracking financial activities of networks, provided that they are related to material flows[137]. Furthermore, rights to make house searches, access to premises and documents and seizure possibilities granted to them are valuable assets in the effort to characterize networks to the extent that they can cross-reference, verify and document information that might originate from various sources.

TRACFIN (processing of intelligence and action against clandestine financial systems)[138] is responsible for receiving financial information from the private sector in France and cross-referencing it with other sources available to it. Apart from civil servants in the Ministry of Finance and Customs, the organization includes agents from the Ministries of Defense and the Interior. The unit also has a right to communicate and exchange information with foreign services with similar competences. Nevertheless, the activity of TRACFIN is limited to detection of operations taking place within France.

On the contrary, the *Office of Terrorism and Financial Intelligence* (OTFI) within the United States Treasury Department in 2004 was created within the logic of a struggle against transnational financial flows[139]. Beyond intelligence missions, this organization has legal powers within the framework of two specific provisions:

- *Executive Order* 13382 June 28 2005 ("*Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters*") enables the Justice, Treasury and State Departments to prohibit any transaction between the United States and persons or companies participating in proliferation activities[140]. Section 5 allows the

[136] http://www.douane.gouv.fr/page.asp ?id=501
[137] Interview notes.
[138] http://www.tracfin.minefi.gouv.fr/informations.htm
[139] « Prepared Remarks by Stuart Levey, Undersecretary for Terrorism and Financial Intelligence before the American Enterprise Institute », September 8, 2006.
[140] http://www.fas.org/irp/offdocs/eo/eo-13382.htm

Treasury Department to use these powers without prior notification to the persons concerned.

- Section 311 of the 2001 *Patriot Act* enables the Secretary to the Treasury to cutoff a foreign institution identified as being *of primary money laundering concern*, from the American economic system.

In order to complete its missions, this body has special tools designed to monitor international financial flows. In particular, obtaining targeted data output from the SWIFT (Society for Worldwide Interbank Financial Telecommunication) is apparently included in this arsenal[141]. Furthermore, the functional concentration of financial security activities within the Treasury Department enables the OTFI to use all services potentially concerned, including services carrying out intelligence or financial repression activities[142].

Therefore although their fields of competence are different, the various existing intelligence services provide States with complementary capabilities for monitoring and warning concerning:

- Persons and companies operating within and outside the country involved in proliferation activities; the national surveillance activity appears to be essential, and in particular it detects acquisition attempts undertaken by networks[143] but it also creates a map of intermediaries and companies contacted or used for proliferation purposes. Another objective is to make private players aware of questions related to proliferation. This approach encourages involvement of the commercial sector in the proliferation alert and monitoring system. This is particularly important because companies targeted by proliferation networks can be economically vulnerable and therefore inclined to be less rigorous towards their potential customers.
- Programs of proliferation players; determining the situation of development efforts of proliferation players is a compulsory passage point to combat networks supplying them. Detailed knowledge must make it possible to determine the fields in which a specific network will look for external support. However, reaching such a level is more complex in nuclear and missile programs since they are often considered as being strategic, and important security measures are taken for them. The case of the Iraqi military biological program, that Baghdad had successfully kept secret until 1995 despite the powers assigned to the special United Nations commission, shows the difficulties that intelligence services can face. In conclusion, it appears possible to obtain not more than a general overview of progress of a program, and possibly precise information about some of its aspects.
- Material or immaterial transfers of sensitive technologies; monitoring of attempts to acquire, export or transport sensitive technologies represents an important part of the activity of intelligence services. In reality, a distinction has to be made between intelligence related to operations carried out from the country for which the final objective may be neutralization of a branch or agents working for the network, and intelligence related to overseas transactions that participate in an enterprise to map

[141] « Prepared Remarks by Stuart Levey, Undersecretary for Terrorism and Financial Intelligence before the American Enterprise Institute », September 8, 2006.
[142] Author's Interviews, November 2006.
[143] Between 2003 and 2004, the British MI-5 indicated that it had contributed to blocking 30 acquisition attempts made by "countries of concern". http://www.mi5.gov.uk/output/Page161.html

network activities. In fact, the latter objective may have two purposes, depending on whether information obtained is shared with allied services[144] or is used to build up national knowledge about a network.

2.1.2 –Adaptation of intelligence tools to challenges created by proliferation networks

Therefore, existing systems in the West can detect flows of material and persons involved in proliferation traffic, at least within their own countries.

However, globalization of the operation of proliferation organizations and the emergence of networks of networks raise the problem of cooperation between national services. Although intelligence exchanges made between Western services appear to achieve a satisfactory level of cooperation for monitoring of persons and material transactions[145], this is not obviously the case for intelligence services of States directly involved in proliferation traffic. Thus, to say the least, the degree of Pakistan's cooperation in mapping the Khan network, as it continues to financially maintain a network of companies and intermediaries for its acquisition network[146], should be considered in relative terms. It is difficult to imagine that Islamabad has provided all the information it possesses, knowing that some agents in the Khan network are probably still working for it. Cooperation of States acting as platforms for some traffic also raises the problem of the economic value of the activities involved. For example, for a country such as Singapore, protection of its financial interests involves a search for a compromise between transparency towards its allies and protection of the confidentiality of company activities.

We also need to question the capacity for detection and monitoring of immaterial technology flows. In this respect, the development of tools for globally monitoring dematerialized exchanges is still in its infancy. Although the United States has made efforts to control its own companies[147], we are still far from setting up a worldwide capacity for monitoring (and processing) of data passing through telephone and computer networks[148]. Nevertheless, progress made in the field of information technologies has made interception of telephone and electronic communications of an identified person easier. In this respect, the combined use of intelligence derived from human sources and from technical sources should at least partly facilitate performance of this mission.

---

[144] To alert them about an activity taking place on their territory or to increase common knowledge. The United States set up two programs (*Golden sentry* and *blue lantern*), designed to verify the end use of goods exported to allied countries with the objective of verifying a priori the nature of the end user or the declared use. For illustration, see http://www.dsca.mil/sc_conf_2002/Golden%20Sentry%20(Leon%20Yates).ppt

[145] Either in bilateral form or multilaterally within control regimes, initiatives to set up bans or NATO.

[146] For example, see http://www.armscontrolwonk.com/820/companies-and-organisations-of-proliferation-concern

[147] B. Gruselle, « Cruise missiles and anti-access strategies», FRS study, December 2005, p. 50.

[148] However, setting up such a capacity is not technically impossible. For example, the Internet system is based on a few thousand relay stations (routers) directing information traffic between servers connected to the network. In theory, installation of interception systems at these routers could be used to monitor exchanges on the web. However, note that the biggest difficulty is related to processing of the information thus obtained. http://computer.howstuffworks.com/router.htm/printable

This comment is also applicable to financial flows, particularly flows made electronically. Thus, apparently in the Banco Delta Asia case, data transmission through SWIFT was used to cross-check information available to American intelligence services. This involved accessing precise information using legally enforceable writs rather than monitoring all data managed by SWIFT, as shown by the company's press release[149] and various declarations of the Treasury Department.

Thus, in the field of monitoring of immaterial and financial flows, intelligence services potentially have tools that they can use to extend existing systems for monitoring flows of equipment and persons. However, in order to make the best use of these tools, intelligence systems need reliable and precise data originating from human sources including agents, foreign services and the private sector.

2.1.3 – *Improve the efficiency of intelligence tools faced with the proliferation networks*

Two methods should be given priority to improve the efficiency of intelligence tools in the detection and surveillance of proliferation networks:

- Broaden and increase international cooperation between intelligence services; this is probably the most difficult task due to political, security and even economic problems that can be raised by intelligence exchanges. A first step could consist of extending exchanges between services within large multilateral regimes to include monitoring and control of material, immaterial and financial flows. In setting up a discussion forum specifically for control experts in 2002, the Missile Technology Control Regime (MTCR) contributed to the policy of strengthening dialog about methods used by proliferation networks and even handling of specific cases[150]. This type of forum also contributes to creating links between experts and effectively facilitating bilateral exchanges. In financing, the Egmont group created in 1995 to coordinate intelligence organizations, also includes an operational work group (composed particularly of services from Singapore, the United Arab Emirates, and Malaysia) that has adopted the same logic[151]. Apparently, the new *Proliferation Security Initiative* (PSI) and particularly the *Container Security Initiative* (CSI) has contributed to increasing exchanges between services in participating countries, and particularly between these services and United States Services[152]. In general, development of cooperation and bilateral customs assistance provides an efficient means of strengthening operational intelligence exchanges between the countries involved. This development is particularly useful for broadening this type of exchanges with countries playing a central role in logistic operations of networks, for example such as transshipment countries.
- Increase the involvement of the private sector in the detection of network activities: industrial or service companies, bank or financial institutions and intermediaries play important roles in the operation and procurement of proliferation networks. The

[149] http://www.swift.com/index.cfm ?item_id=59897
[150] http://www.bis.doc.gov/News/2003/AnnualReport/chapter5p. pdf#search=%22mtcr%20information%20exchange%20enforcement%22
[151] http://www.egmontgroup. org/asia.html
[152] As a reminder, ports that signed CSI agreements with the United States accept the presence of American Customs units that can request inspection of a given container based on national information. For example, see State Department, « Container Security Initiative Now Operational in Singapore », March 18, 2003.

involvement of most of them is based solely on economic interests and usually on poor knowledge of their client and/or the possible use of goods, services or technologies that they will supply. It is then essential to get these players more closely involved in State efforts against proliferation networks. The particular objective in terms of intelligence is to enlist the commitment of companies to report any suspicious operations in which these companies might be involved. Such an obligation already exists in France for banking and financial institutions as part of the struggle against money laundering, but its extension to the remainder of the commercial sector is still limited. Several reasons can be advanced to explain this:

- ⇨ The number of companies concerned: as we have seen, proliferation networks are increasingly trying to acquire elementary components, broadening the pallet of technical activities concerned and therefore the number of companies likely to be targeted. An awareness and information operation needs to be carried out by administrations responsible for controlling dual-use goods, in an attempt to enlist the assistance of these companies. It has been found that it is practically impossible to draw up a precise map of companies producing dual goods in the lack of any formal administrative registration procedure[153].
- ⇨ The size and economic situation of companies; very small companies are particularly attractive targets for networks and their agents in that they are often dependent on a limited number of projects for their survival and economic dependence. This dependence makes them less attentive to the nature of the client, the sensitivity of the goods concerned and setting up of unusual routing circuits. This trend is further strengthened by the absence of punishment or the low fines incurred if control legislation in force is circumvented. Public application of severe sanctions not only acts as a deterrent, but also improves awareness[154]. In this respect, adoption and strict application of "catch all" type legislation appears to be the best solution because it transfers responsibility for checking that the goods that a company wants to sell and/or its final destination are not sensitive, to this company[155].

Therefore efforts to improve the intelligence tool to make it more effective against proliferation networks should work towards the development of a close relation between these intelligence services and small sensitive companies. The first step necessary to achieve this is to draw up an exhaustive list of companies potentially concerned, and to keep it up to date. Introduction of catch all type mechanisms into the national legislation can facilitate this process by encouraging companies to work more closely with official services. The next step is to define the nature of exchanges between companies and intelligence services. Considering the example of TRACFIN, the unit receives declarations of suspicion but it also sends feedback to the declaring company in two forms: firstly to notify it that its declaration is processed, and secondly targeted or untargeted training, information and actions to increase awareness. Similarly, the American Treasury Department provides information to financial institutions complementary to publicity actions around cases for which repressive measures have

[153] Like that which authorizes companies to make or market military equipment.

[154] The potential publicity about financial repression or export control exercised by the American administration helps to make the sectors concerned aware of the fact that circumventing of existing rules, or their habitual laxism in their knowledge about their customer, will have a non-negligible economic impact. Interviews in Washington, November 2006.

[155] We will consider "catch all" type clauses in more detail in the remainder of the study.

been taken[156]. Finally, it seems essential to make all necessary efforts to build up a successful dialog between private players and intelligence services.

2.2 – Neutralization of networks: means, limits and prospects

Durably neutralizing proliferation networks is the main objective in the struggle against proliferation. An admittedly imperfect map of these networks (structure, functional organization) can be drawn up even before this work starts, making use of available intelligence. Several types of tools could be imagined to achieve this result, including financial, economic, police and legal tools. But due to the international structure of proliferation networks, these tools can only be effective if they are adopted by the largest possible number of States. Therefore, it appears important to start by recapitulating the existing international legal bases that could facilitate this harmonization.

2.2.1 –International bases for the struggle against proliferation networks

By adopting Resolution 1540 on April 28 2004, the United Nations Security Council placed the foundation stone for the international struggle against proliferation networks, based on chapter VII in the Charter. In its preamble, the resolution poses the problem in these terms: "*seriously concerned by the threat consisting of the traffic of nuclear, chemical or biological weapons and their vectors, and* ***related elements***[157], *that adds a new dimension to the question of proliferation of these weapons and also creates threat to peace and international stability*". Therefore, one of the purposes of this resolution is to reduce the traffic of goods, technologies and know how in the nuclear and missile fields. It also emphasizes the need to prevent non-state players from accessing this type of weapon.

The Security Council imposes several types of measures on United Nations members that may have a direct impact on the operation of networks:

1. Banning of illegal intermediation activities for weapons, vectors and related elements; this is the purpose of point c) in article 3 in particular, that imposes that measures should be taken to detect, deter, prevent and combat intermediation.
2. Control of final users: point d) in the article deals essentially with control over transit and transshipment, but it also obliges States to set up means for controlling the nature of the final user.
3. The control of services and funds for export operations; this same point also obliges States to control "*the supply of funds or services (for example financing or transport) related to export or transshipment operations that would contribute to proliferation*".

However, in terms of services, it is unfortunate that resolution 1540 does no more than request control over services related to exports. Some networks use intermediary banks

[156] Author's Interviews, November 2006.

[157] The author added the bold characters. The resolution defines the related elements as follows: materials, equipment and technologies covered by treaties and relevant multilateral arrangements or included on national control lists that could be used for the design, development, manufacturing or use of nuclear, chemical or biological weapons and their vectors.

and financing institutions in the country in which they are operating, without them being involved in export operations.

Another resolution of the Security Council corrects this omission, but only in the special case of North Korea. Resolution 1695 adopted on July 15 2006 targets Pyongyang's supply and acquisition activities directly. Section 4 in particular requires Member states to apply enhanced vigilance to prevent the acquisition of missiles, technologies and goods related to missiles and weapons of mass destruction from North Korea. It adds that this effort must also apply to **any financial transfer** related to non-conventional North Korean programs[158].

The international legal framework defined by resolution 1540 deserves to be improved, particularly using lines fixed by the text of the resolution related to North Korean non-conventional programs. However, even if the Security Council succeeds in agreeing upon a better targeted text, it is improbable that it will be applied universally. On the other hand, progressive extension of the principles of the struggle against proliferation networks to source States[159] through *ad hoc* initiatives or multi-lateral groups appears to be feasible. Thus, extension of the *Proliferation Security Initiative* to cooperation between police forces deserves further exploration[160]. Its purpose would be to facilitate national investigations carried out on persons or organizations related to the networks, through the exchange of information and facilitation of extradition measures.

However, note that the application field of resolution 1540 remains very limited. It is restricted to criminalizing proliferation of non-conventional weapons by non-state players[161]. Consequently, even if the text is intentionally ambiguous concerning proliferation of States, its extension to this case appears politically improbable because some countries are legally carrying out activities for the development of nuclear weapons and even more so of missiles.

Resolution 1718 voted on October 14 2006[162] after the North Korean test on October 9 2006, could become a standard for the struggle against proliferation networks. Apart from freezing North Korean credits, its article 8.d states that States must prevent their nationals and persons acting on their land from providing financial support to any person or entity involved in North Korean missile or nuclear programs. Article 8.f also decrees that any freight entering or leaving the country must be searched. Apart from its virtue as an example for future or ongoing proliferation matters, application of this resolution could help to improve methods used by some service companies that now directly support the functioning of networks, including bank institutions and also transport and freight businesses[163]. In particular, application of this resolution could make companies concerned more vigilant with regard to the nature of their clients'

[158] http://daccessdds.un.org/doc/UNDOC/GEN/N06/431/65/PDF/N0643165.pdf ?OpenElement

[159] This is the term used to refer to States in which companies whose proliferation networks are attempting to acquire goods or technologies are located. By extension, it also includes tax havens, States flying convenience flags and countries acting as turntables for traffic.

[160] J. Caves, « Globalization and WMD Proliferation Networks: the Policy Landscape », *Strategic Insights*, op. cit.

[161] See articles 1 and 2.

[162] Under chapter VII.

[163] Author's Interviews, November 2006.

activities and possibly strengthen dialog between the private sector and services and agencies responsible for the struggle against proliferation[164].

2.2.2 – *Tools used in the struggle against proliferation networks*

Thus, setting up multi-lateral organizations must make it possible to coordinate the policies of source States in the struggle against networks. Therefore, such tools must include States that produce technologies and also States sheltering service activities[165] that might be used by the organizations working in the business of weapons of mass destruction.

Therefore, the role of these tools is to design means of durably neutralizing the most fragile key functions of networks, these functions having been identified in advance by intelligence efforts. Two comments should be made:

1. The internal part of networks, in other words the part that operates with no contact with the outside can only be dismantled through a political action aimed at bending the will of the proliferation player (or the States that support it) to continue its activities. Thus, Pakistani authorities needed to take action to neutralize the engineering function of the Khan network.
2. Neutralization of one function is not always enough to dismantle the network. Although this may be the case for star networks, particular strategies have to be adopted for cyclic or informal networks. In these latter cases, dismantling will be effectively achieved either if all functions are neutralized, or if all connections between them are broken[166].

Consequently, preventing the activities of proliferation networks must be based on a set of complementary measures designed to affect all their functions and operational links. In particular:

- prevent financial movements between banks dependent on the network, intermediary banks and local banks;
- neutralize intermediaries, agents and front companies operating for the network;
- hinder production and movements of goods made for the network[167].

Although its action at the moment is concentrated on money laundering and financing of terrorism, the Financial Action Task Force (FATF) is the most suitable setting to coordinate the struggle against financing of proliferation. In fact, the adoption of resolution 1540 would effectively extend its field of action to include this category. The FATF was created by the G-7 in 1989 and now includes 33 member countries[168], this core being supplemented by observer countries and the existence of regional forums (for example a Pacific-Asian group including China) and the participation of international agencies and organizations. The FATF has made 40 recommendations offering the framework of concerted international action on financing of proliferation traffic,

[164] See §2.1.3.
[165] Financing, transport/charter, transshipment, intermediation.
[166] Alexander H. Montgomery, « Ringing in Proliferation », op. cit., p. 170.
[167] This point will be developed in the following chapter
[168] For the list of members, see http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html#FATF_Members

particularly because these recommendations are recognized by the World Bank and the International Monetary Fund[169].

FATF recommendations apply essentially to two domains:

Firstly, the need for States to have a legal framework within which they can prosecute persons or legal entities involved in laundering activities. It must include temporary measures (freezing or seizure) or permanent measures (confiscation) aimed at laundered goods, income originating from laundering and the instruments used for this infraction. Such a recommendation could be extended to the repression of financial activities of proliferation networks, as was done for repression of terrorist group financial activities.

Furthermore, the FATF proposes several methods of reinforcing the role of financial institutions in the struggle against money laundering and financing of terrorism that could be useful against the financing of proliferation. In particular, the objective is to oblige financial institutions to identify and check the activities of their customers and bank institutions with which they set up relations. If there is any doubt, they are requested to decline the clientele of the person concerned or the creation of links with the bank. Bank institutions are also requested to be particularly vigilant about capital movements by electronic means and unusual operations. The FATF also invites States to set up a system for declaration of all national and international cash transactions exceeding a certain amount. Such a measure would strike proliferation networks directly, since they often need to reinject cash funds into the banking system.

Extension of the recommendations made by the Financial Action Task Force to include financing of proliferation networks is an interesting approach to create the first basis for action against these networks. The existence of two Security Council resolutions concerning criminalization of proliferation could form the basis for such an extension. However, questions should be asked about the feasibility of such an initiative, knowing that some countries linked to the FATF (as is the case for China and also Pakistan) now participate in proliferation activities and could be victims of an extension to recommendations. Furthermore, the application scope of Resolution 1540 at the moment is limited to non-state players. Its extension to proliferation by States raises difficult problems, particularly for missiles for which there is no treaty or ban convention. However, since these States rely on structures or persons that are not directly related to them for their acquisitions, it appears feasible to target these structures or persons without opening the question of the rights of States. In other words, it appears possible to extend the role of the FATF to include the struggle against the underground part of proliferation.

In addition to setting up an international policy to resist financing of proliferation, we need to consider measures aimed at the economic players used by networks. In particular, they must be capable of neutralizing intermediaries used by the networks to make contact with their targeted companies. Although supplier groups (MTCR, NSG and Wassenaar) appear to have made commitments to discussions and coordination in this field[170], States are still relatively inactive. Except for the United States that introduced measures aimed at intermediaries in 1996 in the law on control of weapon

[169] For the FATF recommendations, see http://www.fatf-gafi.org/dataoecd/7/55/34850891.PDF

[170] See the press release for the 20th plenary meeting of the missile technologies control regime: http://www.mtcr.info/english/press/madrid.html

exports[171], few countries have legal instruments aimed at brokers[172]. However in 2003, the European Union Council adopted a common position on control of armament intermediaries[173]. In both cases, the objective was to:

- List brokers operating within the territory concerned. Setting up an activity authorization system is sometimes considered as being one of the best means of controlling operators.
- Obliging intermediaries to obtain prior authorization for each operation in which they are involved.
- Set up a legal system to punish unauthorized intermediation activities.

Considering the transnational nature of intermediaries' activities and their geographic mobility, it would appear at first sight that no solution to the involvement of this business in proliferation could be found without international control over this business. Obviously, it is very improbable that this could ever be achieved. Yet as we have seen, brokers cannot fully benefit from this freedom and need local relations in order to carry out their operations. Furthermore, this business is characterized by the diversity of the projects handled, the brokers' activity essentially being guided by customers' needs. Paradoxically, it seems likely that if they were faced with a choice between their local set up and a part of their business, most intermediaries would abandon their illegal activities. Thus, if neighboring groups of countries set up coherent laws about brokering of non-conventional weapons, the role of commercial intermediaries in operation of the networks would probably be reduced. They would also have an effect for agents operating exclusively for the benefit of proliferation networks, making their activity illegal. Therefore, it appears essential that source States, and particularly Western states, should quickly pass legislation to control the intermediation activity in the field of complete systems and also for dual-use goods associated with them, in accordance with resolution 1540.

In conclusion, although multilateral tools appear to be used in financing to contribute to the struggle against proliferation networks, it appears necessary to improve tools used for neutralization of intermediaries and agents acting on behalf of these networks. In particular, Western States should adopt legal measures to control activities of brokers dealing with weapons of mass destruction and associated goods and technologies, as quickly as possible.

2.2.3 – What changes are possible to control flows of goods and technologies?

The capability of States to effectively prohibit exports from their country of goods or technologies coveted by networks is probably one of the main tools useful to neutralize networks activity in the long term. For example, if Malaysian authorities had been capable of preventing the delivery of parts made by the SCOPE Company to the Khan network, the Khan network would probably have found it difficult to fulfill the Libyan

[171] Loretta Bondy, « The US law on arms brokering in 11 questions and answers », presentation to UN workshop in preparation of consultations on illegal brokering, May 2005.
[172] Note that the US law makes authorization of brokering compulsory for all citizens in the United States regardless of the country in which they are located.
[173] EU Council, « Position on control of weapons intermediaries », 2003/468/CFSP, June 23 2003.

order. As we have already mentioned, suppliers and acquisition networks depend on external industrial suppliers to achieve their purposes.

In most countries, material and immaterial flows are controlled based on a coherent set of means and measures[174], themselves based on the existence of **lists of goods and technologies** for which export and transit are usually governed by obtaining prior authorizations issued by the authorities. Consequently, production of effective lists is a central means in terms of flow controls.

This is the case particularly for lists related to dual-use goods. In particular, complete systems and their main components are usually relatively well controlled. There is only a small number of manufacturers capable of assembling or producing them, consequently these companies and the national authorities are aware of their sensitivity.

On the other hand, production of lists of dual-use goods and especially keeping them up-to-date are difficult tasks considering the continuing change in technologies[175]. The main difficulty of such an approach based solely on the existence of lists is in the control application. For a country with limited administrative resources[176], the amount of work involved in management of applications for export or transit of dual-use goods may become such that it leads to malfunctions in their processing: delays, superficial analyses, errors, etc. Similarly, uninformed or badly informed manufacturers, or manufacturers who do not accept responsibility for their actions, could easily produce incomplete or unusable applications.

Several alternatives could be considered to improve control over dual-use goods and prevent problems of an approach based solely on use of these lists.

Setting up "catch all" clauses partly satisfies this problem. The objective is no longer to evaluate the intrinsic sensitivity of a particular product, but rather to identify the sensitivity of the customer receiving the product and the use that he might make of it[177]. Catch all clauses also make it compulsory for exporters to inform control authorities if they have any suspicion about the end use of the product or the nature of the final user, thus contributing to increasing the responsibility of companies[178] (in the same way as for control over financial flows). In fact, it is impossible to imagine such increased responsibility without informing and training companies. Apart from training of company executives, it might also be useful to publish a regular report on violations of control rules[179].

Apart from the adoption of "catch all" clauses, the possibility of producing final destination lists should be considered. Despite the political difficulties that might hinder their creation, such documents have a genuine advantage as part of the struggle against

[174] In particular, physical or documentation controls that can take place before or at the time of export. The United States also continues controls after export and monitors exported goods.
[175] This can be proven simply by looking at the lists of goods produced by the Wassenaar arrangement.
[176] These are precisely the countries that we might like to be most vigilant in terms of controls, because they are the main targets of networks operatives.
[177] Irina Albrecht, « Catch-all controls », paper prepared for the International Control Conference, London, 2004.
[178] Ibid. For an example declaration of suspicion
see: https ://www.bis.doc.gov/forms/eeleadsntips.html
[179] The industrial security office in the American trade department responsible for control of exports of dual-use goods publishes a document of this type annually. For the year 2006,
see http://www.bis.doc.gov/ComplianceAndEnforcement/Majorcaselist.pdf

proliferation networks, provided that sufficient prior intelligence work has been done to map their structure. This is true particularly because production of this type of document is quite possible within multinational groups[180] in order to better coordinate the efforts of a group of countries.

Setting up a global policy to deliberately limit the dissemination of proliferation technologies deserves further exploration. In 2004, President Bush made a speech to the *National Defense University*[181] proposing to prevent States who did not possess enrichment and reprocessing technologies from acquiring them. Despite the disagreements following this proposal, we have demonstrated that dissemination of technologies facilitates action of proliferation networks and consequently limiting this dissemination would probably make their task more difficult. This comment is equally true for technologies related to the fuel cycle[182] and the technologies used for example for space launchers. This type of proposal would have the merit of reducing the risk of seeing new structured networks developing capable of supplying a complete product. But it would only be valid if it were accompanied by globalization (and hardening) of control measures for elementary components, in particular dual-use components.

2.3 – Action by armed forces and limitation of proliferation flows

The tools and methods described above are aimed essentially at neutralizing a network as a whole, starting from the moment at which its structure and organization have sufficient vulnerabilities to be exploited. In practice, it is impossible to neutralize some of the structure of state networks[183]. Undoubtedly, attempts can be made to neutralize their agents, to slow down their financial flows or to make their access difficult to suppliers. But everything suggests that these networks can continue to operate firstly in degraded mode and then possibly normally, by turning towards less strict suppliers or intermediaries located in States with more lax controls.

In this case, considering the considerable risk that arises if these networks are able to access the goods and technologies that they are looking for, our policies should make targeted actions on specific transactions so as to prevent them. Furthermore, it appears necessary to query whether or not other solutions might be used involving military means that could affect the internal part of these networks, even indirectly.

Start up of the Proliferation Security Initiative (PSI) in May 2003 created the necessary setting for international cooperation between the armed forces of participating countries in order to allow interception and searching of suspicious cargos. Despite its legal weaknesses[184], the main advantages of this initiative are that it can stop material flows of proliferation goods although they are no longer in an area for which member countries are responsible, and particularly in international spaces. Thus, this initiative provides a partial solution to the weakness of some national control systems. But the PSI cannot operate unless the mapping work already mentioned in the previous chapters has been

[180] For example, groups of suppliers: MTCR, NSG.

[181] President Georges W. Bush, « Remarks by the President on Weapons of Mass Destruction Proliferation », National Defense University, February 11th, 2004.

[182] Some States have already announced their intention to resume or to begin enrichment activities with declared civil end purposes.

[183] See § 2.2.2 in this document.

[184] B. Gruselle, « Cruise missiles and anti-access strategies», op. cit., p. 48.

done. As mentioned by President Bush in February 2004 during his speech to the *National Defense University*:

> "*This picture of the Khan network was pieced together over several years by American and British intelligence officers. Our intelligence services gradually uncovered this network's reach, and identified its key experts and agents and money men. Operatives followed its transactions, mapped the extent of its operations. They monitored the travel of A. Q. Khan and senior associates. They shadowed members of the network around the world, they recorded their conversations, they penetrated their operations, we've uncovered their secrets.*"

Therefore, the German ship *BBC China* and the parts made by SCOPE for the network could be stopped and examined in October 2003[185] as a result of the prior intelligence work; incidentally exposing the activities of A.Q. Khan and unraveling (at least partly) the network that he was managing.

Ban operations appear to serve two purposes in the struggle against proliferation networks:

- Occasionally prevent the delivery of goods: even if the investigation of the network is not finished, in some specific cases it may be essential to prevent acquisition of goods. For example, this may be applicable to the delivery of key components for production of the system considered or the will to neutralize part of the system.
- Complete an investigation in order to expose an entire network; for public diplomatic purposes, it may be useful to complete an investigation on a network by making a ban. This principle is illustrated in the case of the *BBC China* that acted both as a preamble for dismantling the Khan network[186], but also provided a message contributing towards the negotiation between Libya, the United States and the United Kingdom.

Despite its successes, the Proliferation Security Initiative (PSI) remains a fragile structure. In particular, since it is not an international organization, it is tributary to any political changes at the head of the States participating in it[187]. No doubt the initiative would disintegrate if the United States progressively decides to abandon it. Without achieving institutionalization solutions that would probably make the system less efficient in the long term, the PSI should be put into a more formal setting. One of the solutions could be to enact the major principles in a United Nations Security Council resolution complementary to Resolution 1540[188]. Even if this could reduce the margin for maneuver of PSI member countries, at least the principle of the struggle against proliferation networks would be registered in a universal text.

In the short term, an improvement to the military and political aspects of the PSI would undoubtedly involve extending its scope. Search and seizure operations are only possible within a very strict setting; authorization of the State in which the vessel is

[185] http://www.carnegieendowment.org/publications/index.cfm ?fa=view&id=17420&prog=zgp&proj=znpp

[186] Once again, we would like to emphasize the fact that this dismantling is neither final nor complete. However, it is *a priori* a considerable success in efforts to control networks.

[187] David Albright & Corey Hinderstein, « Unraveling the A. Q. Khan and Future Proliferation Networks », op. cit., p. 123.

[188] See above for principles of extension to resolution 1540.

registered[189], or within the framework of legal rights of States within their territorial area. This creates the problem of how to ban vessels registered in a non-cooperating State and traveling in international spaces. There are two possible ways of improving the system:

- On an *ad hoc* basis: i.e. a specific resolution made by the Security Council to authorize member countries of the United Nations to intercept vessels belonging to a State in international waters. In reality, this would be more applicable to preparation of a resolution dealing with a specific proliferation problem – like the case for resolution 1718 on North Korea or a possible future resolution on Iran – to authorize States to search a ship or an aircraft belonging to the country concerned. However, the feasibility of this type of approach is by no means certain considering the reticence of China and Russia to adopt sanctions for proliferation affairs.
- Systematic and if possible complete search of any vehicle in a Proliferation State passing through the territorial area of PSI countries[190]. Such a provision could be complemented if required by bans on stopovers or transshipments for the vessels considered.

Furthermore, broadening of the PSI's action framework to include other aspects of the struggle against proliferation networks deserves further study. Everything suggests that the American administration might want to extend this initiative to include the struggle against financial flows related to proliferation[191]. Nevertheless for the moment, the PSI is no more than a tool that facilitates cooperation between military forces about bans on movements of goods. It would be useful to set up a high level coordination and decision making authority composed of the players concerned, so as to maintain the coherence of the initiative while extending it.

Beyond the use of armed forces for ban operations, the direct use of force against persons controlling networks is worth examining. Without going as far as the regime change, setting up clandestine operations against internal parts of the networks could provide one way of reducing their efficiency, and in some cases even neutralizing them in the long term. With reference to the Iraqi example, neutralization of persons coordinating MIC's and the secret services' work would probably have reduced the capability of the network to operate efficiently. The legal, technical and political conditions under which actions against members of a network can be undertaken should be considered in more detail, although this does raise legal problems.

[189] In general, based on a bilateral agreement

[190] A systematic search of any vessel leaving the territorial space of a State could be envisaged, for example in the framework of an *ad hoc* resolution of the Security Council like that taken against North Korea after the October 9th, 2006 test.

[191] Author's Interviews, November 2006.

Armed preventive action against state programs also has to be considered. Note that the *Iraqi Freedom* operation, apart from permanently neutralizing the Iraqi network, presumably made it possible to precipitate Libya's decision to renounce its nuclear ambitions. Apart from the massive use of force with the objective of overturning proliferators that, in the short term, does not appear very credible due to the situation of American armed forces[192], targeted actions – which would not need as much logistic – could have an adverse effect on activities of the networks and programs that they supply.

[192] J. Caves, « Globalization and WMD Proliferation Networks: The Policy Landscape », op. cit.

Conclusion

The two examples that were analyzed in detail in this study (Abdul Qader Khan's network and the Iraqi acquisition organization) illustrate the functional and organizational principles that apparently control the structure of most existing proliferation networks.

In particular, the result is the importance of coordination between management of financial and physical flows and technical expertise, in other words knowledge of sold and purchased systems and components. Thus networks cannot function well unless they are capable of discretely moving funds used to pay the various parties concerned, selecting goods required by users, and routing them to these users. To achieve this, they are using their own agents (persons, companies or financial institutions) as well as a series of participants (banks, suppliers and service companies) who do not know or do not wish to find out who they are working for.

It should also be emphasized that networks have been able to take full advantage of the increase in world trade and its consequences. They have taken advantage of the dissemination of technologies to obtain supplies from companies located in countries that do not have export control systems. Similarly, they were capable of dissimulating their financial and physical flows by increasing the number of intermediaries and front companies and dematerializing their movements of funds.

Nevertheless, "globalization" also forms a potential source of risk for functioning of proliferation networks. The increasing dependence of companies and banks on the world market makes them sensitive to sanctions that would cut them off from the world market. Thus, measures taken by the American Treasury department to prohibit access of *Banco Delta Asia* to the American market led this bank to freeze North Korean credits that it was managing. Furthermore, the publicity around these measures could create a domino effect on a broader set of companies potentially concerned, or even on the States in which they are located. These States are also faced with increasing constraints in terms of controls on exports and material flows passing through their territory that they must respect so as not to be commercially penalized. This leads to the beginning of tighter control practices by countries such as Dubai or Singapore that had been used as logistic platforms by the networks.

In any case, all that we can do at the moment is to state the need to set up or reinforce existing tools to struggle against proliferation networks. The first step in the effort to organize such an approach should be to produce an overall policy to coordinate intelligence actions, repression tools and ban means. Each of these aspects will play a particular and unique role towards achieving long-term neutralization of proliferation networks:

- Mapping the structure and organization, detect operations and monitor flows.
- Permanently neutralize agents, suppliers and key intermediaries.
- Interrupt material and immaterial flows at chosen moments.

In particular, the objective is to achieve a compromise between long-term actions to dismantle an organization, and short-term operations that can be useful from a security

point of view but might compromise long-term operations. Strategies in the struggle against proliferation networks are adapted to each specific case and should follow three main principles:

- Interrupt financial flows between banks belonging to the network and external financial institutions.
- Concentrate repression measures on intermediaries and front companies.
- Neutralize logistic activities (production and movement).

Therefore, the struggle against proliferation networks must include international cooperation and cooperation between different government bodies in each country, and it must also be based on strengthened cooperation between the administrations concerned and the industrial and financial world. Fast progress is now being made on financial aspects. In particular, it has become essential to upgrade tools for the struggle against illegal financial flows, to deal with the problem of financing of proliferation networks. Extending the mandate of the Financial Action Task Force (FATF) to include the question of proliferation traffic could reinforce international cooperation, both in intelligence and in neutralization of networks' agents. Possible tracks could also be explored to improve adaptation of export control systems to the struggle against proliferation networks. Targeted measures should be applied to intermediaries, because they have become key elements for functioning of networks. In particular, coherent laws governing brokering and making it illegal for non-conventional weapons need to be set up.

Finally, the United Nations Security Council's adoption of Resolution 1540 and especially Resolution 1718 that targets North Korean activities, sets the foundations for coordinated international action against physical and financial proliferation flows. Although at first sight the *Proliferation Security Initiative* provides an attractive framework for coordination of international action considering its degree of progress, its essentially military nature makes it unsuitable for this mission. In any case, the durability of this authority that is very dependent on investment by the American Administration is uncertain. Therefore, means of formalizing its operational framework should be considered in more detail before extending its competence to include coordination of repression actions.

BIBLIOGRAPHY

- "The Diffusion of Military Technologies and Ideas", Published by Emily O. Goldman & Leslie C. Eliason, Stanford University Press, 2003
- Chaim Braun & Christopher F. Chyba, "Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime", *International Security*, Vol. 29, n° 2 (Fall 2004)
- Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network", *International Security*, Vol. 30, n° 2 (Fall 2005)
- Michael Eisenstadt, "Iraq and After: Taking the Right Lessons for Combating Weapons of Mass Destruction", Center for the Study of Weapons of Mass Destruction, Occasional Paper 2, National Defense University Press, May 2005.
- Lewis A. Dunn, "The Changing Face of Proliferation: Some thoughts, Speculations, and Provocations", CSIS-SANDIA Workshop, February 2005.
- "Globalization and WMD Proliferation Networks: Challenges to US Security", Naval Postgraduate School, Conference Report, July 2005.
- "Black Markets, Loopholes, and Trade Controls", Carnegie Endowment for International Peace, Roundtable transcript, November 2005.
- Anne Plats Barrow, Paul Kucik, William Skimmyhorn, John Straigis, "A System Analysis of the A. Q. Khan Network", University of Stanford, Social Science Seminar, December 2005.
- Sammy Salama, Lydia Hansell, "Companies reported to Have Sold or Attempted to Sell Libya Gas Centrifuge Component", Center for Nonproliferation Studies, March 2005.
- Press Release by the Inspector General of Police, Malaysia, "In Relation to Investigation on the Alleged Production of Components for Libya's Uranium Enrichment Programme", Released February 20, 2004.
- Iraqi Survey Group Final Report, September 30, 2004.
- David Albright and Corey Hinderstein, "Unraveling the A. Q. Khan and Future Proliferation Networks", *The Washington Quarterly*, Spring 2005.
- John P. Caves Jr, "Globalization and WMD Proliferation Networks: The Policy Landscape", *Strategic Insights*, Vol. V, Issue 6, June 2006.