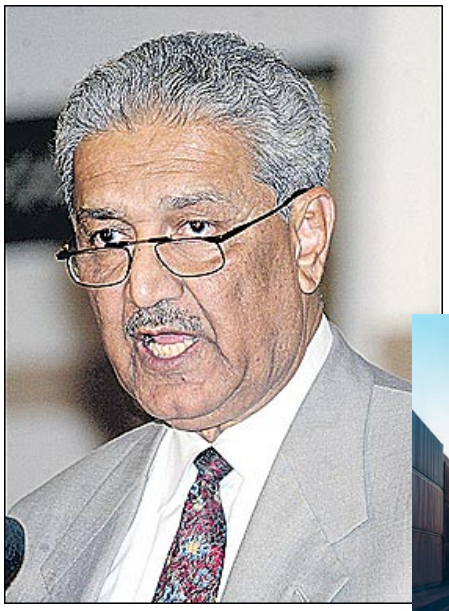
Fondation pour la Recherche Stratégique

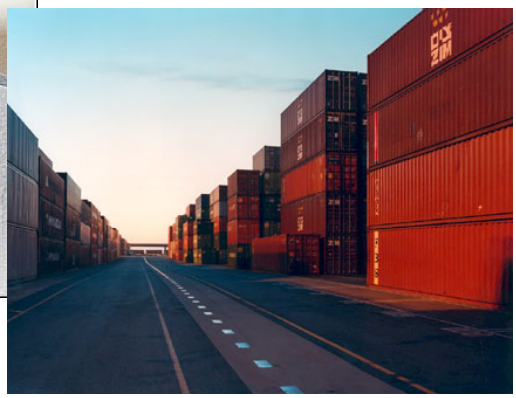
Recherches & Documents

# Réseaux et financement de la prolifération

Bruno Gruselle

(3 mars 2007)





Fondation pour la Recherche Stratégique • 27, rue Damesme • 75013 PARIS
Tél. : 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

# SOMMAIRE

## Introduction

L'interception du navire allemand *BBC China* en octobre 2003, débouchant sur la découverte de plusieurs dizaines d'éléments de centrifugeuses à destination de la Libye, a permis de dévoiler l'existence d'un réseau de trafic de technologies nucléaires de grande ampleur. Son fondateur, le Dr Abdul Qader Khan, considéré comme le père de la bombe nucléaire pakistanaise, en utilisant les contacts tissés dans le cadre de ce programme, était parvenu à créer une machine commerciale destinée à assister, contre rémunération, les pays aspirants à la possession de l'arme nucléaire dans leur quête.

Cette entreprise illustre l'apparition d'un phénomène de prolifération secondaire – *second-tier proliferation* – dans lequel les pays en développement s'assistent mutuellement dans leurs efforts pour développer et posséder des armes nucléaires ou encore des missiles[1]. En effet, tout porte à croire que le réseau Khan s'étendait au-delà de la seule assistance à des programmes nucléaires et a contribué à la mise en place de coopérations techniques entre ses clients. C'est le cas par exemple de la mise au point du missile Nodong et de ses variantes pakistanaises (Ghauri) et iraniennes (Shahab-3).

Bien que l'attention se soit focalisée sur le réseau Khan, l'existence de plusieurs systèmes plus ou moins enchevêtrés, mis en place pour contourner l'édifice de non-prolifération ne fait pas de doute. Les travaux réalisés par l'*Iraqi Survey Group* démontent celui que l'Irak de Saddam Hussein avait mis en place pour contourner l'embargo et acquérir à l'étranger des biens destinés à des programmes prohibés. De même, les activités mafieuses du régime nord-coréen incluent vraisemblablement la fourniture de technologies proliférantes à des clients comme l'Iran, le Pakistan ou encore la Syrie. D'autres réseaux de prolifération, comme celui qui a conduit le transfert de missiles Kh-65 à l'Iran et à la République Populaire de Chine, s'apparentent davantage à des entreprises criminelles « classiques » s'appuyant sur les faiblesses des systèmes de contrôle.

Le développement et l'évolution de ces réseaux, dont certains existent déjà depuis quelques décennies, traduisent plusieurs tendances lourdes en matière de prolifération.

D'une part, les outils de contrôle mis en place par certains États s'avèrent efficaces pour empêcher l'acquisition de technologies clefs des domaines nucléaire et missile. *A contrario*, les évolutions techniques ont tendance à banaliser certains biens anciennement réservés au domaine militaire. Parallèlement, le spectre des technologies et des outils potentiellement utilisables pour des projets proliférants connaît un élargissement rapide. Les États occidentaux font littéralement face à une explosion de la quantité de biens et de services qui devraient faire l'objet de contrôle du fait de leur possible application à des programmes nucléaires ou de missiles : il suffit d'observer l'évolution récente des listes de biens duaux contrôlés par les régimes de fournisseurs pour se convaincre de l'ampleur de la tâche des instances nationales de contrôle.

En outre, la diffusion mondiale de certaines de ces technologies – pour des applications *a priori* légitimes – rend presque impossible un contrôle strict de leur destination. L'implication de la société malaisienne SCOPE dans le réseau Khan illustre la difficulté : dans un pays où il n'existe que peu voire pas de contrôle rigoureux des transferts de

[1] C. Baum & C. F. Chyba, « Proliferation Rings », *International Security*, Vol. 29, n° 2, Fall 2004, p. 5.

biens sensibles, une société peut librement produire et exporter des biens sans savoir qu'ils sont destinés à un programme nucléaire[2]. Ainsi, la qualité hétéroclite des systèmes de contrôle nationaux permet aux réseaux de prolifération d'acquérir auprès de certains pays les biens que les membres des régimes de fournisseurs leur refusent.

L'essor des échanges mondiaux, tant matériels qu'immatériels, a eu tendance à faciliter cette tâche.

Les principaux points de transit du commerce mondial, comme Dubaï ou encore Singapour, qui traitent d'importants volumes de transactions sans avoir développé de dispositif de contrôle adéquat, ont été massivement exploités par les proliférants comme plaques tournantes pour les flux matériels, en particulier par l'implantation locale de sociétés écrans chargées de gérer à la fois l'acquisition de biens duaux en Occident et leur acheminement vers leur destination finale.

Le développement des moyens de communication – Internet ou encore les supports légers capables de stocker d'importantes quantités de données – a permis aux fournisseurs de transférer presqu'impunément des savoir-faire à leur client, voire de délocaliser une partie du soutien technique aux programmes. D'autre part dans le domaine académique, l'essor des coopérations scientifiques ou encore l'accélération de politiques de formation à l'étranger ont contribué directement à l'accroissement du niveau technique des cadres susceptibles de participer à des programmes nucléaires ou de missiles.

Enfin, force est de constater que, paradoxalement, le phénomène de prolifération s'est privatisé. Si certains États impliqués directement dans la fourniture de biens proliférants ont officiellement renoncé à cette activité, les réseaux existants continuent de fonctionner plus ou moins indépendamment. Dans les cas chinois ou pakistanais, se pose en effet la question du degré de complicité des administrations voire des instances dirigeantes.

Pour les proliférants, ces tendances ont une conséquence pratique : si les savoir-faire critiques sont plus difficiles à obtenir car mieux protégés par les pays détenteurs, la majeure partie des biens nécessaires au développement d'un programme est accessible. En mettant à profit les outils de la mondialisation économique, les réseaux de prolifération peuvent plus facilement parvenir à l'un de leur principal objectif à savoir contourner les dispositifs d'interdiction afin d'approvisionner leur client.

## VERS UNE MODELISATION DES RESEAUX DE PROLIFERATION

Pour parvenir aux technologies dont ils ont besoin, les acteurs proliférants doivent être en mesure :

- d'accéder aux composants duaux via l'acquisition discrète (directe ou non) ;
- d'obtenir les savoir-faire critiques[3] et de les assimiler.

Deux voies s'offrent à eux pour y parvenir :

- Créer un outil d'acquisition nationale, adossé à un effort de développement autonome ou quasi-autonome. Le cas irakien correspond à ce cas de figure : le réseau d'acqui-

[2] Rapport de l'enquête malaisienne sur les activités de B.S.A. Tahir et de SCOPE, 20 février 2004.

[3] Qu'il s'agisse de connaissances empiriques ou acquises à travers l'expérience. Cf. Alexander H. Montgomery, « Ringing in Proliferation », in *International Security*, Vol. 30, n° 2, Fall 2005, p. 176.

sition remplit des fonctions logistiques, financières et administratives mais n'est pas directement impliqué dans l'effort technique.

➥ Faire appel à un fournisseur extérieur capable de transférer les savoir-faire critiques, voire de fournir une capacité clef en main, en proposant une série de services techniques et commerciaux complémentaires. En particulier, il doit être en mesure de participer à l'évaluation technique du besoin et à l'élaboration d'une offre, de garantir le transfert des biens matériels et immatériels associés, et de les intégrer au profit du client. C'est le cas du réseau Khan ou encore du système de transfert de technologies de missiles nord-coréen.

La frontière entre fournisseurs et acheteurs s'avère toutefois poreuse. Un réseau d'acquisition peut être amené à devenir pourvoyeur de technologies. A titre d'exemple, l'existence d'une transaction « Nodong pour centrifugeuses » entre le réseau nord-coréen et le réseau Khan est évoquée[4]. De même, le réseau nucléaire pakistanais bâtit dans les années 1970 pour soutenir l'effort d'Islamabad en matière d'acquisition est devenu le premier « SuperU de la prolifération »[5].

Pour pouvoir dégager des solutions adaptées à cette nouvelle ère de la prolifération, une étude systémique de leur fonctionnement s'impose. Il s'agira tout d'abord d'identifier la structure des deux grands types de réseaux : principales fonctions remplies, méthodes employées pour la gestion des flux (financiers, de biens, de savoirs). A partir des deux cas d'école les mieux documentés, le réseau Khan et le système irakien, il est possible d'identifier les mécanismes clefs qui structurent les réseaux tant d'acquisition que de fournisseurs.

Il s'agira ensuite de modéliser les deux grands types de réseaux de prolifération. Enfin, il restera à tirer des conclusions sur les conditions de fonctionnement des réseaux et donc sur leurs vulnérabilités.

## PERMETTRE LE CHOIX DE SOLUTIONS ADAPTEES POUR REPONDRE AU DEVELOPPEMENT DES RESEAUX

Face à des systèmes bâtis pour exploiter les failles du cadre traditionnel de non-prolifération, qu'il s'agisse de traités ou de régimes, la communauté de sécurité se doit de concevoir des solutions spécifiques.

Les efforts américains en la matière ont reçu une large publicité : outils internationaux (PSI), accords bilatéraux (CSI, *Megaports*) ou encore initiatives nationales (contrôle des flux immatériels, mise sous embargo d'établissements bancaires, surveillance des étudiants étrangers). Et ils ont fait l'objet de nombreuses critiques tant sur la forme que sur le fond.

Sans revenir sur les supposées arrière-pensées de Washington, il convient de s'attacher à analyser la pertinence des solutions existantes par rapport au phénomène observé et d'apporter des éléments de jugement sur leur exhaustivité et leur limite.

[4] Gaurav Kampani, « Second Tier Proliferation: The Case of Pakistan and North Korea », *Nonproliferation Review*, Vol. 9, n° 3, Fall/Winter 2002.

[5] Traduction libre de « *nuclear WalMart* ».

L'objectif de l'étude est de proposer des solutions pratiques destinées à compléter et à renforcer le dispositif existant. En particulier, les outils de gestion des flux tant financiers, matériels qu'immatériels méritent que l'on s'y attarde dans la mesure où, par rapport aux entreprises terroristes dans lesquelles ils sont en première analyse faibles, les fonds comme les matériels considérés dans les phénomènes de prolifération sont importants[6].

En outre, la faisabilité économique et politique de certaines mesures d'incitation positives doit également faire l'objet d'une réflexion tant elles apparaissent complémentaires d'approches davantage répressives.

[6] Le commerce balistique nord-coréen rapporterait annuellement à Pyongyang entre 500 millions et 1 milliard de dollars.

## 1 – Analyse systémique des réseaux de fournisseurs et de demandeurs

Il n'existe pas un cheminement unique qui conduise à l'apparition de réseaux de prolifération. Chaque outil mis en place par des acteurs pour acquérir ou fournir des biens proliférants est spécifique et répond à des contraintes et à des besoins liés à l'environnement immédiat – politique, sécuritaire, économique et culturel – des programmes qu'il alimente[7]. Les principaux déterminants qui président à l'apparition de tels réseaux restent toutefois globalement identiques, même si les situations individuelles des acteurs concernés varient. Ainsi, il paraît possible, en première analyse, d'en citer deux essentiels :

- La volonté de détenir des armes nucléaires et leurs moyens d'emport.
- L'impossibilité d'accéder aux biens requis de façon légitime et/ou légale.

L'existence d'une demande forte de la part de certains États a toujours constitué le principal moteur de la prolifération, mais la structuration des réseaux destinés à y répondre est nouvelle. Elle a été rendue possible par trois phénomènes concomitants.

En premier lieu, l'accroissement des flux de commerce mondiaux et l'essor des outils pour les gérer permettent de mieux dissimuler les transferts matériels et immatériels. Les réseaux de prolifération, comme d'autres organisations de trafic, se nichent dans les coins sombres d'un commerce mondial devenu difficile à surveiller avec rigueur[8]. Le laxisme de certains États en matière de contrôle est largement exploité à travers le recours à des sociétés écrans ou encore par l'utilisation d'intermédiaires techniques ou financiers, pour réaliser ou régler les transferts.

D'autre part, la banalisation de certaines technologies et biens, autrefois spécifiques de programmes militaires, permet aux proliférants et aux prolifératrices de tromper la vigilance des autorités chargées du contrôle de la prolifération. Enfin, l'apparition de fournisseurs capables et désireux de transférer aux acheteurs potentiels des systèmes complets et les technologies associées constitue l'un des facteurs déclenchant de la mise en place de ces nouveaux réseaux de prolifération. A ce titre, le cas des exportations balistiques nord-coréennes est symptomatique d'autant qu'il s'intègre dans un ensemble d'activités criminelles destinées à financer la nomenklatura[9].

Ainsi, les opérations du réseau Khan ou l'adaptation du système d'acquisition irakien illustrent les tendances en matière de flux de prolifération. L'un comme l'autre sont assez étendus et leurs opérations assez connues pour nous permettre de comprendre pratiquement leur fonctionnement et de pouvoir en tirer des conclusions sur la structuration de ce type d'organisation.

---

[7] On peut parler de facteurs d'incitation et de freins (*incentives and disincentives*). Voir « *The Diffusion of Military Technologies and Ideas* », Edited by Emily O. Goldman & Leslie C. Eliason, Standford University Press, 2003, p. 163.

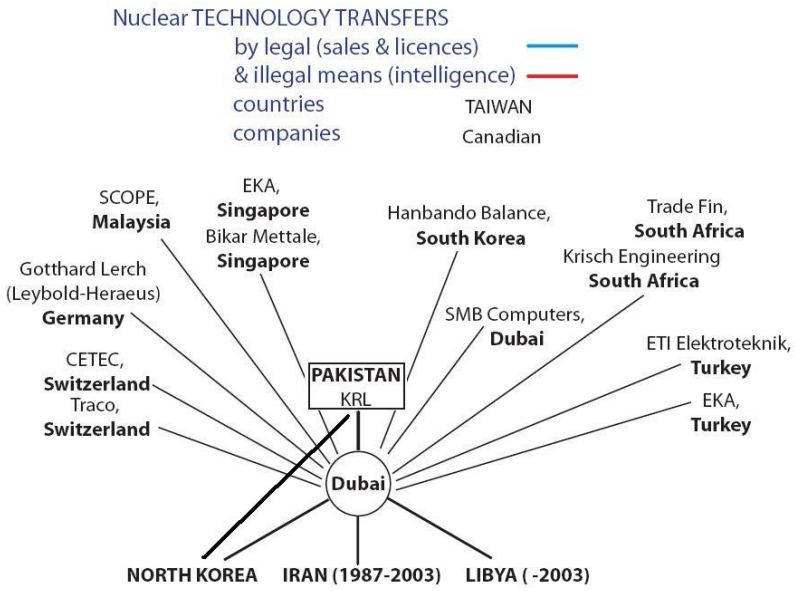
[8] « Globalization and WMD Proliferation Networks: Challenges to US Security », Naval Postgraduate School, Conference Report, July 2005.

[9] Pêle-mêle ces activités comprennent le trafic de fausses devises, de drogues ou encore la contrefaçon.

## *1.1 – Etudes de cas*

### *1.1.1 – Fournisseurs : Le réseau A. Q. Khan*

➡ **Historique**




Constitué dans les années 1970 pour permettre au Pakistan de développer son programme nucléaire militaire afin de répondre à l'essai mené par les Indiens en 1974, le réseau d'acquisition pakistanais s'est appuyé en particulier sur l'une des figures de ce programme : le Dr Abdul Qader Khan.

Fournisseurs, intermédiaires et contacts scientifiques et techniques, rencontrés lors de démarches visant à la fois à maîtriser le cycle du combustible et à obtenir des plans d'armes nucléaires, étaient personnellement liés à A. Q. Khan. Ces relations personnelles constituent sans doute l'une des principales caractéristiques du réseau pakistanais. Ainsi, le Sri Lankais Buhary Seyed Abu Tahir (BSA Tahir), qui semble avoir été le bras droit de Khan au sein du réseau, aurait rencontré ce dernier dans le cadre de la fourniture aux *Kahuta Research Laboratory* (KRL) de moyens de climatisation[10]. Les autres personnes physiques membres du réseau avaient également eu l'occasion de coopérer avec Khan dans le cadre du programme nucléaire pakistanais.

L'utilisation de ce réseau à des fins d'exportation/ventes de technologies nucléaires semble se dessiner dès le milieu des années 1980. A cette époque, l'organisation de Khan est sans doute encore intégrée à un ensemble plus vaste sous le contrôle de l'État pakistanais. Tout porte à croire que ce n'est qu'à partir du milieu des années 1990 que Khan va progressivement détacher une partie de l'organisation pour travailler à son seul profit. Ce nouveau réseau privé, que BSA Tahir qualifiera d'organisation informelle (« *loose organization* »[11]), va définitivement s'autonomiser à partir de 1999.

La première affaire connue du réseau de fourniture pakistanais remonte donc au milieu des années 1980. A cette époque, Khan aurait en effet pris des contacts avec l'Iran pour la fourniture de plans de centrifugeuses. L'affaire se conclut en 1994-1995, quand BSA Tahir est chargé par A. Q. Khan du transfert de centrifugeuses depuis le Pakistan vers l'Iran via sa société, SMB Group, installée à Dubaï. Cette transaction, d'un montant de

[10] Voir le compte-rendu de l'enquête menée par les services de police malais. 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.

3 millions de dollars, aurait été réglée par les Iraniens par un versement en liquide à BSA Tahir en dirham des Émirats Arabes Unis.

Des contacts auraient également été pris avec l'Irak avant la première guerre du Golfe pour la fourniture de plans d'arme ainsi que de technologies de centrifugation[12]. Selon les informations disponibles, les services de sécurité irakiens (SSI) n'auraient pas donné suite aux premiers entretiens avec les représentants de Khan. Toutefois, une réunion préliminaire se serait tenue fin 1990 en Grèce, au cours de laquelle un agent appartenant au réseau aurait proposé le recours à un intermédiaire dubaiote pour l'acquisition de certains biens en Occident. En termes financiers, cet agent aurait demandé une commission de 10 % pour chacune des acquisitions effectuées en Occident s'ajoutant à une somme forfaitaire de 5 millions de dollars pour l'ensemble de l'opération.

Les contacts entre le réseau Khan et la Corée du Nord ont, quant à eux, débuté dans le cadre de la relation officielle tissée entre Islamabad et Pyongyang à la fin des années 1980. Suite à la visite de Benazir Buttho en Corée en décembre 1993, la coopération semble s'être matérialisée à travers le transfert de la technologie des missiles Nodong au Pakistan. Les *Khan Research Laboratories* (KRL), alors en compétition avec le *Pakistan Atomic Energy Commission* sur le programme nucléaire, sont placés au cœur de la relation avec Pyongyang. Outre la vente de quelques dizaines de missiles complets et d'au moins un lanceur[13], le Pakistan obtient du régime communiste le transfert de savoir-faire, de technologie et la construction d'un site d'assemblage. Grâce au soutien nord-coréen, le Pakistan procède le 6 avril 1998 au premier tir du missile Ghauri. Or, selon les révélations d' A. Q. Khan[14], son réseau entreprend à partir de 1997 de livrer à Pyongyang la capacité d'enrichissement d'uranium, de l'hexafluorure d'uranium (UF6), ainsi que des plans d'arme, livrés directement depuis le Pakistan[15]. Un soutien technique était également assuré par le personnel des KRL sur requête nord-coréenne. Même si ces transferts ont été effectués, comme le prétendent les autorités pakistanaises, hors du contrôle du gouvernement, nul doute qu'ils ont été rendus possibles par le rôle central occupé par les KRL et Khan lui-même dans la coopération balistique. En outre, les affirmations officielles pakistanaises se heurtent à la question de la contrepartie pakistanaise aux transferts nord-coréens.

En effet, dans la période concernée, la situation économique du Pakistan est fortement dégradée : croissance faible, inflation forte (aux alentours de 10 %), forte dette,

[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] Les estimations varient entre 12 et 25 missiles. Joseph S. Bermudez, « A History of Ballistic Missile Development in the DPRK », CNS Occasional Papers n° 2, 1999, pp. 23-24.

[14] C. Braun & C. F. Chyba, « Proliferation Rings : New Challenges to the Nuclear Nonproliferation Regime », *International Security*, Vol. 29, n° 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
Il convient également de noter la possible complicité de la République Populaire de Chine dans la facilitation des transferts physiques : « *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

investissements en diminution, productivité faible[16]. Elle ne commencera à s'améliorer qu'à partir de 2000-2001, sous l'influence des réformes engagées par Pervez Musharraf sous la pression du Fonds Monétaire International et de la Banque Mondiale. En clair, le Pakistan n'est pas à l'époque en état de financer des acquisitions balistiques auprès d'un pays qui considère ses programmes comme une source primordiale de devises. Il est bien entendu difficile d'évaluer exactement le montant de la transaction, mais si l'on suppose un prix unitaire d'environ 4 millions de dollars par missiles[17], soit environ 40 millions pour l'ensemble, auxquels il convient d'ajouter les commissions pour le transfert de technologies et l'implantation de capacités de production. De façon réaliste, on peut estimer le montant total à une centaine de millions de dollars, dont la Corée du Nord aurait exigé le versement rapide et complet vu sa propre situation économique et les impératifs clientélistes du régime. En définitive, le principe d'un troc paraît plausible, même si le fait que A. Q. Khan ait encaissé une commission paraît vraisemblable, dans la mesure où cette somme correspond globalement à celle exigée par lui pour une livraison similaire en Libye[18].

A partir de 1997, la Libye contacte également le réseau Khan afin d'acquérir des capacités d'enrichissement d'uranium à des fins militaires[19]. Les premières réunions, auxquelles assiste BSA Tahir, se déroulent en Turquie, au Maroc et à Dubaï. A partir de 2001, le réseau Khan entreprend plusieurs opérations pour répondre au besoin de son client :

- La livraison de 1,7 tonne d'hexafluorure d'uranium : le transport est effectué par voie aérienne depuis le Pakistan. Cette transaction est financièrement séparée des autres.
- La fourniture de centrifugeuses de types P-1 et P-2, assemblées ou en kit. Deux cents centrifugeuses P-1, deux de type P-2 et plusieurs dizaines de composants pour des centrifugeuses de type P-2 seront livrés directement depuis le Pakistan.
- La construction d'un atelier de fabrication pour des composants de centrifugeuses (Project Machine Shop-1001/projet 1001).
- La fourniture de plans d'arme nucléaire.

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

[17] « Seoul details N. Korea's Taepodong-2 ties to Iran, calls missiles main cash source », *East-Asia Intel,* August 9, 2006. Le prix unitaire d'un système Nodong est évalué à 4 millions de dollars.

[18] Cf. infra.

[19] Sammy Salama & Lydia Hansell, « Companies Reported to Have Sold or Attempted to Sell Libye Gas Centrifuge Components », Center for Nonproliferation Studies, March 2005.

Ces opérations sont coordonnées par Khan et leur montant total atteint quelques centaines de millions de dollars. L'une d'entre elles est particulièrement significative dans la mesure où elle fait appel au réseau tissé par Khan depuis les années 1970-80. Le projet 1001, dont BSA Tahir est le principal organisateur et le trésorier, nécessite en effet que le réseau puisse transférer et construire de façon discrète une usine de fabrication de composants pour centrifugeuses en Libye, mais également qu'il puisse développer une capacité pérenne d'approvisionnement pour le programme. Pour ce faire, deux filières indépendantes seront utilisées :

- L'une, impliquant entre autres un ressortissant britannique, Peter Griffin, est chargée d'acheter en Europe des machines-outils et des moyens de production (four à vide) et d'assurer la formation des techniciens libyens à l'utilisation de ces machines[20].
- L'autre, structurée autour de plusieurs membres de la famille Tinner, des ressortissants sud-africains ayant participé au programme nucléaire de Pretoria ainsi que des entreprises dans plusieurs pays, devait fournir des composants clefs pour l'assemblage des centrifugeuses. Une partie de ces composants, dont les enveloppes des centrifuges, seront produits – sur la base de plans fournis par le réseau – par une société malaisienne *Scomi Precision Engineering* (SCOPE). Urs Tinner est détaché à partir d'avril 2002 jusqu'à octobre 2003 auprès de SCOPE, pour assister à la fabrication des pièces qui devront être livrées à la Libye via une société dubaïote. Pour SCOPE, les composants produits avaient pour destinataire final les Émirats Arabes Unis dans le cadre des activités pétrolières[21]. Pour les besoins de cette opération, SCOPE était amené à importer, depuis la filiale singapourienne de Bikar Mettal, des barres et des cylindres d'aluminium en grande quantité. L'interception d'une cargaison de composants provenant de SCOPE, à bord du navire allemand *BBC China* à destination de la Libye, le 4 octobre 2003, a conduit au démantèlement de l'opération. L'approvisionnement du programme libyen devait également être assuré par des sociétés dirigées par des relations de Khan, situées en Suisse, en Allemagne, en Turquie et en Afrique du Sud.

### ➧ L'organisation du réseau Khan

Au centre du réseau se trouve une série d'hommes de confiance rencontrés par A. Q. Khan dans le cadre du programme nucléaire pakistanais et des activités d'acquisition qu'il dirigeait. Pour autant c'est bien A. Q. Khan qui jouait le rôle clef dans l'organisation du réseau, à la fois en tant que coordinateur et comme autorité technique. Tout porte à croire qu'il a exploité le potentiel des KRL pour soutenir techniquement son réseau[22], c'est-à-dire se mettre en situation de proposer des offres complètes incluant la maîtrise de l'ensemble du cycle d'enrichissement. De même, Khan a su exploiter ses contacts au sein de l'administration pakistanaise pour pouvoir exporter sans restriction certains produits sensibles à ses clients, en particulier des centrifugeuses appartenant au programme nucléaire. Il est difficile de croire que cette activité a pu être menée sans que les autorités politiques du pays n'en soient conscientes.

[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.

[21] Ibid.

[22] Plusieurs de ses proches au sein des laboratoires ont été arrêtés au Pakistan en 2003.

L'autonomie dont a bénéficié Khan dans le cadre du programme nucléaire pakistanais et des efforts clandestins d'acquisition peut expliquer en partie la facilité avec laquelle le réseau a pu réorienter discrètement ses activités vers la fourniture. Il apparaît toutefois invraisemblable que les services de sécurité pakistanais [ISI] n'aient pas eu vent des trafics de Khan. L'épisode nord-coréen donne à penser que les autorités politiques et militaires ont *a minima* laissé faire dans l'intérêt des programmes stratégiques du pays. Khan apparaît également comme le commercial du réseau, participant à plusieurs réunions avec ses clients.

Le Sri Lankais Buhary Seyed Abu Tahir (BSA Tahir) semble être devenu, dans les années 1994-1995, le principal facilitateur des affaires du réseau alors que celui-ci en traitait un nombre croissant. A travers le contrôle de sociétés installées à Dubaï, en particulier le groupe SMB dont il est le directeur depuis 1985, BSA Tahir a pu coordonner les transactions générées par l'entreprise de Khan. Son rôle dans le réseau comprenait également le montage et l'utilisation de compagnies écrans, destinées à faciliter le transit des biens vers les clients, et la gestion des divers intermédiaires et fournisseurs impliqués dans les trafics[23]. Ainsi, c'est BSA Tahir qui semble avoir été chargé de rémunérer les sociétés travaillant au profit du réseau, que ce soit celles, comme SCOPE, qui ont été instrumentalisées, ou celles qui connaissaient l'objet des opérations. Si certaines opérations semblent avoir été réglées en liquide, d'autres ont fait l'objet de virements internationaux dans le cadre de contrats dûment établis. C'est le cas, par exemple, du contrat passé entre la société *Gulf Technical Industries* (GTI) et SCOPE, pour un montant de 13 millions de dollars[24]. Ce rôle de responsable financier et logistique semble confirmé par sa présence aux entretiens entre Khan et les clients du réseau, ainsi que par ses contacts privilégiés avec les autres membres de celui-ci[25].

Suivant les affaires traitées, d'autres consultants ont été amenés à intervenir au profit du réseau, soit pour établir des sociétés écrans, soit pour fournir du matériel, soit encore pour mener à bien une opération particulière. Il ne semble pas toutefois qu'ils aient eu un rôle permanent dans les activités du réseau mais plutôt qu'ils étaient chargés ponctuellement de remplir une mission. C'est le cas de Peter Griffin, d'abord pressenti pour prendre en charge les travaux de SCOPE au profit du client libyen puis écarté au profit de Urs Tinner. Pour chaque opération, tout porte à croire que le réseau Khan était organisé ponctuellement pour répondre à la demande. Ainsi, Gotthard Lerch, que Khan avait connu dans les années 1970 en Europe, aurait été en charge de l'opération libyenne et directement responsable pour la coordination de la branche sud-africaine[26].

Plusieurs sociétés ont également joué un rôle central dans le réseau pakistanais, volontairement ou non. Outre l'implication ponctuelle de certaines dans le cadre d'affaires

[23] Sammy Salama & Lydia Hansell, « Companies Reported to Have Sold or Attempted to Sell Libye Gas Centrifuge Components », op. cit.

[24] Michael Laufer, « A. Q. Khan Nuclear Chronology », Carnegie Endowment for International Peace, Proliferation Brief, Vol. 8, n° 8, September 2005, p. 7.

[25] « Companies Reported to Have Sold or Attempted to Sell Libye Gas Centrifuge Components », op. cit.

[26] « Network of Death on Trial », *Der Spiegel*, 13 mars 2006 (traduction http://service.spiegel.de/cache/international/spiegel/0,1518,druck-405847,00.html)

données, d'autres semblent avoir contribué directement au fonctionnement du réseau. On peut *grosso modo* identifier trois types d'entreprises selon leur rôle :

- Les sociétés écrans, installées pour l'essentiel à Dubaï, ont été utilisées pour l'acquisition auprès de fournisseurs ou d'intermédiaires de matériels en dissimulant le destinataire final des biens. C'est le cas par exemple de *Gulf Technical Industries* ou de SMB. Ces sociétés ont, outre leur rôle occasionnel au sein du réseau, des activités commerciales et/ou industrielles normales et existent généralement depuis plusieurs années[27]. La création de « coquilles vides » pour des opérations spécifiques est souvent évoquée mais aucune donnée précise ne permet de conclure à leur utilisation systématique.
- Les intermédiaires, qu'il s'agisse de sociétés ou de personnes physiques, jouent un rôle central dans l'approvisionnement du réseau. Les principaux intermédiaires du réseau Khan, établis en Europe, en Asie ou en Afrique, avaient pour tâche d'acquérir des composants ou des machines-outils auprès de fournisseurs européens et d'assurer leur acheminement jusqu'aux sociétés écrans dubaïotes. Dans le cas libyen, un intermédiaire sud-africain, Gerhard Wisser, lié aux activités d'acquisition de l'ancien programme nucléaire de Pretoria et ayant des relations historiques avec Khan, est également intervenu pour obtenir certains composants clefs auprès d'une société sud-africaine[28]. Ces intermédiaires de profession étaient rémunérés par le profit des ventes réalisées par le réseau et tout porte à croire qu'ils menaient d'autres activités du même type.
- Les sociétés fournisseurs volontaires ou non. De nombreuses sociétés ont alimenté le réseau Khan en technologies et biens nécessaires à répondre aux besoins de ses clients. Il est frappant de constater que si certaines sont installées dans des pays qui contrôle mal leurs exportations, d'autres, en Europe ou à travers leurs filiales, ont pu être utilisées efficacement pour les besoins du système. En particulier, les intermédiaires ont pu acquérir impunément des machines-outils performantes en Europe et sont parvenus à faire former des techniciens des pays clients pour la mise en œuvre de ces machines[29].

En termes d'organisation financière, les quelques données disponibles pointent sur deux types de transaction :

- Interbancaire : pour la rémunération des agents ou fournisseurs extérieurs au réseau. C'est-à-dire des virements entre les fournisseurs, les intermédiaires[30] et/ou les sociétés écrans. Ainsi, le contrat entre SMB et SCOPE semble avoir été financé de façon classique, probablement à travers des lettres de crédits[31] ou des lettres de change[32].

[27] SMB par exemple a été fondée en 1980 par le père de BSA Tahir, et poursuit des activités dans le domaine des technologies de l'information.

[28] « Companies Reported to Have Sold or Attempted to Sell Libye Gas Centrifuge Components », op. cit.

[29] Voir le rapport d'enquête de la police malaisienne.

[30] Les intermédiaires ont été rémunérés selon toute vraisemblance au titre de contrats industriels.

[31] Lettre de crédit : engagement de la banque émettrice d'effectuer conformément à la demande d'un donneur d'ordre un paiement à un fournisseur sur présentation de documents attestant de l'expédition des marchandises ou de l'exécution d'un contrat.

[32] Lettre de change : document remis par le bénéficiaire au créditeur qui en l'acceptant donne ordre à sa banque de payer la somme indiquée à l'échéance donnée.

- Transactions en liquide[33] à l'intérieur du réseau et avec les clients. Les sommes ainsi obtenues – éventuellement en plusieurs paiements – ont pu ensuite être déposées sur des comptes de pays émergents ou off-shore avant de faire l'objet de transactions interbancaires au profit des bénéficiaires finaux. Même si les paiements étaient effectués en liquide, certaines opérations pourraient avoir fait l'objet de contrats écrits entre Khan (et/ou Tahir) et l'intermédiaire concerné[34].

En ce qui concerne la gestion des flux matériels résultant des opérations du réseau, il semble que trois voies aient été utilisées :

- La livraison directe, depuis le Pakistan et par des moyens nationaux, de centrifugeuses et pièces provenant du stock pakistanais ou d'hexafluorure d'uranium : dans ce cas, l'opération coordonnée directement par Khan implique l'utilisation d'un navire battant pavillon pakistanais ou d'un appareil civil voire militaire pakistanais[35].
- La livraison indirecte depuis le Pakistan via Dubaï : dans ce cas, le matériel est transbordé depuis un navire affrété au Pakistan vers un navire battant pavillon du destinataire final à Dubaï. Ce dernier effectuant la livraison au client sans risque de l'exposer ou d'exposer le réseau.
- La livraison indirecte, par un fournisseur, via Dubaï : ce cas diffère du précédent dans la mesure où l'expéditeur ne connaissant pas la destination finale du bien emprunte tout moyen de transport à sa disposition. Une fois à Dubaï le chargement était transbordé vers un navire battant pavillon de l'État client qui assure la livraison finale.

### ➡ Fonctionnement du réseau

L'entreprise A. Q. Khan semble avoir toujours fonctionné sur le principe d'un contact initial direct entre le chef du réseau et ses clients. Une fois les contacts pris et les grands principes arrêtés – montant de l'opération, nature des fournitures – Khan semble avoir laissé ses principaux associés en charge de la mise en œuvre opérationnelle.

Il existe toutefois une évolution significative entre les marchés iranien et libyen. Dans le premier cas, le rôle des KRL semble avoir été beaucoup plus central, en particulier à travers la fourniture exclusive de biens et des transferts technologiques directement depuis le Pakistan. Dans le second, si les KRL ont continué à jouer un rôle, la gestion opérationnelle des flux de technologies et des échanges financiers a été déléguée à une branche particulière du réseau. Cette évolution tient de façon vraisemblable à la situation personnelle de Khan et à la reprise en main, au moins partielle, de son activité par les autorités militaires du pays après la prise du pouvoir par Musharraf en 1999[36]. Il

[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.

[36] En particulier sa mise à l'écart de la direction des KRL en mars 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*

semble toutefois clair que les services de renseignement pakistanais étaient informés des agissements des KRL, voire qu'ils les ont soutenus au moins jusqu'à l'essai nucléaire de 1998, avec la bénédiction d'une partie de l'establishment politique et militaire[37]. De fait, malgré l'apparition au milieu des années 1990 d'informations mettant en cause les agissements de Khan, en particulier la découverte par l'UNSCOM en 1996 d'un document interne irakien sur l'existence d'un contact entre le programme nucléaire de Bagdad et Khan, il faut attendre 2003 pour que les autorités pakistanaises enquêtent sur le réseau. Le soutien de celles-ci a été l'un des éléments cruciaux pour assurer la continuation des opérations du réseau au même titre que les mesures concrètes prises par Khan pour dissimuler les flux (financiers et physiques) générés par celui-ci tout comme la confidentialité des contacts avec ses clients.

Le fonds de commerce du réseau était avant tout la fourniture d'une offre complète en matière d'enrichissement d'Uranium à des fins militaires. Cette offre était visiblement complétée par l'accès à des plans d'armes compatibles avec la matière fissile, ainsi que la possibilité d'obtenir de l'hexafluorure d'uranium destiné à alimenter le cycle d'enrichissement. En outre, il est parfois fait mention de transferts de savoir-faire concernant le travail de l'uranium métal[38].

L'une des spécificités de ce réseau est d'avoir structuré l'offre en mettant en place un service complet allant de la spécification technique du besoin jusqu'à la livraison finale d'une capacité nucléaire clef en main. Il répondait ainsi à la structure même de la demande et à l'organisation de celle-ci[39], c'est-à-dire la volonté d'acquérir à coup sûr une capacité efficace complète à moindre coût. Cette spécificité doit cependant beaucoup au parcours personnel de Khan et à la façon dont le programme nucléaire pakistanais a été poursuivi. Il apparaît que la tolérance des autorités pakistanaises envers les activités d' A. Q. Khan, ainsi que le mode opératoire retenu pour acquérir les biens et technologies du programme national ont favorisé l'émergence et la consolidation d'une activité privée. On peut donc craindre que les réseaux d'acquisition clandestins des pays proliférants puissent un jour devenir des fournisseurs potentiels d'une offre du même type.

### *1.1.2 – Demandeurs : Le réseau d'acquisition irakien (période 1991-2003)*

#### ➡ Historique et évolutions

Le système irakien d'acquisition de technologies, mis en place à partir de 1991 afin d'alimenter notamment les programmes d'armes non conventionnelles du pays, s'est étoffé et complexifié pour s'adapter au changement de contexte créé par l'apparition du système pétrole contre nourriture.

A partir de 1996, malgré l'embargo imposé par les Nations Unies, le système d'acquisition irakien a su en effet exploiter à la fois la source de revenus de ses ventes de pétrole dans

*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] Cf. infra (réseau irakien).

le cadre et hors du programme pétrole contre nourriture mais également l'ouverture partielle de son marché aux importations pour financer ses opérations et accroître ainsi son réseau de fournisseurs. Celui-ci mêle à la fois des sociétés privées, des intermédiaires, des banques ou encore des fournisseurs volontaires ou non, mais également des gouvernements rémunérés au travers de protocole de fourniture de pétrole[40].

Pour l'essentiel, les tentatives d'acquisition irakiennes à partir de 1991 ont concerné le domaine des missiles – balistiques comme aérobies.

La période allant de 1991 à 1996 a été marquée principalement par des contacts avec des sociétés installées dans trois pays : Roumanie, Ukraine et Jordanie[41]. Alors que les deux premiers ont effectivement été utilisés comme sources de technologies et de biens par l'Irak, le dernier a principalement servi de plaque tournante pour l'ensemble des flux – financiers comme physiques – générés par les activités d'acquisition.

Les contacts avec la société roumaine Aerofina auraient débuté en 1994 par des rencontres avec des experts du domaine du guidage et de la navigation afin d'assister le programme de missile irakien basé sur la modification du SA-2. Des livraisons de matériels, en particulier des moyens d'essai pour les gyroscopes du missile, via la Jordanie, auraient débuté à l'automne 1994 mais se seraient momentanément interrompues en 1995 pour être définitivement stoppées en 1998 à la suite de la découverte de cette opération par l'UNSCOM[42]. Le Comité pour l'Industrialisation Militaire (MIC) aurait également pris des contacts à partir de 2001, à travers des intermédiaires et des sociétés écrans, avec la société Romania Uzinexport pour l'acquisition d'équipements nécessaires à la production d'aimants, susceptibles d'être utilisés pour la fabrication de paliers de centrifugeuses. Il semblerait que l'accord (ou les accords) signé entre les intermédiaires du MIC et la société ait porté sur une assistance pour la fabrication en Irak des aimants. Le montant total de la transaction, payé par une combinaison de fonds en liquide et de lettres de crédits, aurait été de 4,6 millions de dollars[43].

La coopération avec l'Ukraine semble avoir débuté en 1995, au travers de visites officielles relayées par la fourniture de matériels par des sociétés ukrainiennes pour un montant estimé à 140 millions de dollars sur la période 1995-2001[44]. La coopération aurait porté en particulier sur les questions de guidage inertiel au travers de contacts entre Youri Orshansky, directeur de la société MontElect, et les responsables du site d'Al Karama. Ces contacts se seraient également matérialisés par le transfert de systèmes SA-2 complets et de composants de ce missile en 2001 à travers ARMOS, une société écran appartenant au MIC et installée en Russie[45]. Ainsi, l'Irak aurait acquis grâce à MontElect 300 moteurs Volga[46], aurait signé un contrat pour la construction

[40] Bagdad a signé des protocoles de fourniture clandestine de pétrole avec ses voisins : Syrie, Jordanie, Turquie, Yémen et Égypte. Ces protocoles ont été une source de revenus primordiale pour le système clandestin d'acquisitions de l'Irak.

[41] Iraqi Survey Group Final Report, September 30, 2004, p. 87.

[42] Ibid, p. 88.

[43] Cf. infra, pour l'organisation financière du système d'acquisition irakien.

[44] ISG Final Report, p. 89.

[45] Cf. infra.

[46] Il s'agit du moteur du SA-2. L'Irak reconnaît du reste avoir acquis ces moteurs dans le document remis à l'UNMOVIC en décembre 2002.

d'un site de production d'ergols et aurait initié les contacts pour la mise au point d'un banc d'essai au sol.

L'implication de sociétés jordaniennes (ou jordano-irakiennes) dans le système d'acquisition irakien – banques, compagnies écrans et intermédiaires – a débuté dès 1991 et s'est poursuivie jusqu'à 2003. La Jordanie a servi à la fois de plaque tournante pour les importations de matériels, de source de financement à travers le protocole commercial bilatéral et de relais pour les opérations financières du réseau irakien. Le groupe irakien Al Eman[47], l'un des principaux intermédiaires des services secrets irakiens, organisait les flux matériels depuis la Jordanie, y compris le transport des biens jusqu'au destinataire final. En particulier, sa filiale jordanienne aurait dirigé l'acquisition de composants pour le programme Al Samoud, ainsi que de divers biens à double usage dans le domaine de la navigation et de la propulsion, y compris des récepteurs GPS ou des gyroscopes. Au niveau financier, plusieurs banques jordaniennes – en particulier la Banque Nationale de Jordanie – étaient utilisées à la fois pour financer l'activité d'acquisition des intermédiaires irakiens et pour recueillir les fonds illicites provenant de la vente de pétrole. Jusqu'en 1996, 95 % des activités d'acquisition irakiennes étaient conduites par les banques jordaniennes, ce pourcentage diminuant à 30 % après la mise en place du système pétrole contre nourriture.

A partir de 1996, l'Irak a élargi la palette de ses fournisseurs en détournant le système pétrole contre nourriture pour accroître les financements disponibles.

La Syrie a progressivement remplacé la Jordanie comme plaque tournante des trafics irakiens. A partir de la signature de l'accord commercial, en 2000, l'Irak a passé des contrats sous ce protocole pour un montant de 1,2 milliard de dollars[48]. Les importations irakiennes étaient alors directement gérées par une société syrienne, SES International, elle-même en contact avec des sociétés écrans du réseau d'acquisition irakien, en particulier le groupe Al Basha'ir sous le contrôle du MIC, voire directement avec des ministères ou des organisations irakiennes. Dans une moindre mesure, la Turquie est également devenue une source essentielle de revenus pour le réseau irakien à partir de 2000. Générant environ 1 milliard de dollars par an, les divers trafics avec son voisin permettaient d'alimenter les comptes du réseau dans diverses banques de la région : Liban, Turquie, Jordanie.

A partir de la mise en place du système pétrole contre nourriture, le réseau irakien semble avoir tissé de nouveaux liens avec plusieurs sociétés chinoises pour la fourniture de composants dans le domaine du guidage. En particulier, la société chinoise NORINCO aurait été contactée à partir de 2000 pour la fourniture de gyroscopes destinés au programme de missiles irakiens. Même si de nombreux contacts ne semblent pas avoir abouti, la relation entre le réseau irakien et certaines sociétés chinoises semble avoir été florissante en termes de projets[49]. Même si des délégations irakiennes sont entrées directement en contact avec les fournisseurs potentiels, la gestion des flux aurait été

[47] Voir le rapport Duelfer (premier rapport de l'ISG), p. 88. http://www.lib.umich.edu/govdocs/pdf/duelfer1_db.pdf

[48] Il convient de noter que tous ces contrats ne portent pas forcément sur des acquisitions illicites. Selon les données réunies par l'ISG, 186 millions de dollars auraient été consacrés à ce type d'opération. ISG Final Report, p. 94.

[49] ISG Final Report, pp. 102-103.

assurée par les intermédiaires irakiens situés au Proche-Orient et en Asie afin de faciliter l'exportation du matériel vers Bagdad.

Grâce à la relation établie à partir de 1998 avec la firme bulgare JEFF Company, le groupe Al Basha'ir et SES International semblent avoir pu fournir au réseau irakien de nombreux biens nécessaires au développement du programme de missiles et en particulier des machines-outils, ou encore des composants de propergols.

La création en 1998 de la *joint venture* irako-russe ARMOS a permis au réseau d'acquisition irakien de développer ses liens avec Moscou. Bagdad semble avoir également mis à contribution son ambassade à Moscou pour assurer le transport de biens et de fonds entre la Russie, la Syrie et l'Irak. L'Irak aurait surtout utilisé la société ARMOS pour établir des relations avec la société russe Rosoboronexport, laquelle aurait transféré des biens vers l'Irak en utilisant des faux certificats de destination finale établis par les autorités syriennes. La plupart des contrats signés par ARMOS avec des sociétés russes auraient porté sur de l'assistance technique dans le domaine des missiles[50]. Ainsi, la société TECHNOMASH[51] aurait obtenu des contrats pour fournir de l'assistance dans le domaine de la navigation, des structures et pour la construction d'un banc d'essai pour moteurs. ARMOS a également négocié des contrats de fourniture de 280 moteurs Volga au profit de Al Karama en 2002. Ces moteurs, ainsi que d'autres composants pour missiles, ont été transférés depuis la Pologne par un intermédiaire polonais – Ewex Company – au profit la société irakienne Al Basha'ir.

Parmi les divers autres contacts pris par le réseau irakien après 1996, on notera également celui établit en 1999 avec la Corée du Nord. Le MIC aurait cherché en particulier à acquérir auprès de la société nord-coréenne *Changwang Trading Company*[52], des missiles balistiques de longue portée (de type Nodong) ainsi que des missiles antinavires. Plusieurs contrats auraient été signés entre cette société et des entités irakiennes liées au programme Samoud en 2000 et 2001, portant en particulier sur la fourniture de composants nord-coréens. Les paiements étaient effectués par la société syrienne SES International, grâce aux fonds de l'accord commercial Syrie–Irak, directement à l'ambassade de Corée du Nord à Damas[53].

Des sociétés indiennes, biélorusses, taiwanaises et égyptiennes ont également participé à la fourniture de composants au réseau irakien. Dans la plupart des cas, l'utilisation de banques non irakiennes comme relais ainsi que le paiement en liquide par du personnel diplomatique irakien ont constitué la base de la gestion des flux financiers engendrés par les acquisitions irakiennes.

### ➡ L'organisation du réseau irakien

Saddam Hussein se trouvait au plus haut niveau du système d'acquisition irakien, contrôlant le budget consacré aux activités illicites. Ce rôle comprenait en particulier l'établissement d'accords commerciaux avec les pays voisins, servant à la fois comme sources de revenus et comme plaques tournantes pour les flux depuis et vers l'Irak.

[50] ISG Final Report, p. 109.

[51] L'un des principaux bureaux d'étude russes dans le domaine des systèmes spatiaux.

[52] L'une des entités coréennes sanctionnées par l'Administration américaine pour avoir servi d'intermédiaire aux exportations de technologies de missiles de la Corée du Nord.

[53] ISG Final Report, p. 110.

Même si deux organismes, secrétariat présidentiel et Diwan, géraient dans les faits les financements alloués aux projets des organisations demandeuses (services secrets, MIC), la décision finale d'engager ou non des fonds revenait à Saddam Hussein.

La mise en place d'accords commerciaux bilatéraux, après l'adoption du système pétrole contre nourriture, a permis au régime irakien de développer dans les pays signataires son réseau d'acquisition. Ainsi, Bagdad a pu entretenir une série d'intermédiaires industriels et financiers gérant directement les opérations d'acquisition. Les sociétés irakiennes, déjà engagées dans ce type d'activités avant 1996, ont pu établir à l'étranger des succursales contrôlées directement servant de relais aux besoins exprimés par les clients et d'outils pour la gestion des flux financiers et matériels.

Ces sociétés écrans, établies pour certaines dès le début des années 1990, soit par le MIC, soit par les services secrets irakiens, constituaient l'un des moteurs du système irakien et ont été amenées à traiter des centaines d'opérations et à coordonner dans les faits les acquisitions.

Al Basha'ir Trading Company a été ainsi l'une des principales sociétés d'acquisition irakienne. Établie en 1991 et contrôlée par le MIC et probablement les services secrets irakiens, elle a élargi son champ d'activité en établissant plusieurs bureaux régionaux dans les pays servant soit de fournisseurs, soit de plaque tournante au réseau. Ainsi, à partir de 1996, la société contrôle plus de 50 % des activités conduites sous les auspices de l'accord irako-syrien[54], c'est-à-dire une part importante de l'activité d'acquisition irakienne. Cette société participera en particulier, aux côtés de SES International ou de ARCOM, aux négociations avec les fournisseurs d'Europe de l'Est. Al Basha'ir a également servi d'intermédiaire à l'Irak pour la vente illicite de pétrole, bien que cela ne constitue pas le cœur de son activité. Selon les archives de la société pétrolière irakienne SOMO, sa branche jordanienne aurait signé 198 contrats pour la fourniture de produits pétroliers pour un montant total de 15,4 millions de dollars. Créée par le MIC en 2001, la société *Al-Mafakher for Commercial Agencies and Export Company*[55] a conduit quelques opérations mais son volume d'activité est resté moins important que celui d'Al Basha'ir.

Outre l'activité d'acquisition conduite par Al Basha'ir, le régime irakien a encouragé la création de sociétés multinationales sous contrôle de citoyens irakiens. Leurs liens avec les services de sécurité en faisaient des outils privilégiés pour servir à l'étranger l'intérêt du réseau d'acquisition irakien. Ainsi, la société familiale Al Eman, qui possédait des filiales à Dubaï ou encore à Amman, avait un rôle particulier dans les trafics financiers et matériels depuis la Jordanie. En puisant dans les comptes entretenus par les ventes illégales de pétrole, ses filiales assuraient entre autres, la gestion logistique des flux vers l'Irak. En contact permanent avec les attachés commerciaux des ambassades irakiennes (membres des services), les membres de la famille Al Gaood[56] – qui dirigeaient le conglomérat – servaient d'intermédiaires lors des contacts préliminaires avec des fournisseurs potentiels.

Depuis la fin du conflit de 1990-1991, les services de sécurité irakiens (SSI) ont facilité les opérations du réseau d'acquisition. A partir de 1997, la coopération avec le MIC a

[54] ISG Final Report, p. 73.

[55] ISG Final Report, p. 77.

[56] ISG Final Report, pp. 87-89.

permis d'optimiser les activités. Alors que le MIC avait pour charge d'entretenir le réseau d'intermédiaires et de compagnies écrans, à la fois en décidant des fonds alloués et en spécifiant les besoins, les SSI devaient utiliser leurs agents comme :

- Courriers pour des transferts particulièrement sensibles à travers la généralisation de l'utilisation des postes diplomatiques et de la valise pour transporter des biens acquis par le réseau ou des fonds en liquide destinés aux intermédiaires ou fournisseurs. Certaines opérations d'acquisition étaient en outre complètement gérées par les SSI sous la houlette technique du MIC[57].
- Intermédiaires pour l'établissement à l'étranger de compagnies écrans pour le réseau : ces sociétés servaient ponctuellement pour approcher des fournisseurs potentiels et conduire avec eux des transactions. Elles pouvaient à l'occasion être chargées d'assurer l'exportation de biens vers et depuis les plaques tournantes du réseau (Syrie ou Jordanie).
- Facilitateurs pour l'entrée en contrebande de matériel sur le sol irakien : la mise en place d'unités des SSI aux principaux points d'entrée du territoire irakien ou dans les ports de transit devait permettre de faciliter l'entrée par voie terrestre ou maritime des biens acquis par le réseau[58]. En particulier, ces unités étaient chargées par toutes les méthodes possibles d'éviter l'inspection des chargements acquis par le réseau entrant sur le territoire irakien.

De 1990 à 2003, le régime irakien aurait accumulé 10,9 milliards de dollars[59] de revenus illicites par quatre moyens :

- La signature de protocoles commerciaux bilatéraux avec ses principaux voisins et alliés : la principale source de revenus (environ 8 milliards de dollars) reposait sur l'exportation de produits pétroliers en dehors du programme pétrole contre nourriture.
- Des surcoûts appliqués à la vente de pétrole sous le système « pétrole contre nourriture » : à partir de juin 2000, le régime irakien à travers la société d'État SOMO a appliqué aux ventes de pétrole une "taxe" de 25-30 % par baril. Ce surcoût était payé par les clients soit par des versements sur les comptes de SOMO, soit en liquide auprès des missions diplomatiques irakiennes[60]. Le montant obtenu grâce à ce système ce serait élevé à 265 millions de dollars.
- Un système de dessous de table s'appliquant aux importations dans le cadre du programme "pétrole contre nourriture" : les sociétés fournissant des biens à l'Irak étaient assujetties au paiement d'un pourcentage du contrat – environ 10 % – au réseau irakien. La somme était déposée sur un compte bloqué jusqu'au paiement de la livraison puis transférée sur un compte irakien ou celui d'une société écran. Environ 1,5 milliard de dollars de revenus auraient ainsi été générés.
- La vente de produits pétroliers à des sociétés privées en dehors du cadre du programme "pétrole contre nourriture". Cette activité aurait généré environ 1,2 milliard

[57] ISG Final Report, p. 80.

[58] Ce fût le cas en particulier aux points d'entrée surveillés par les inspecteurs du programme pétrole contre nourriture.

[59] ISG Final Report, p. 23.

[60] Ibid, p. 32.

de dollars entre 1991 et 2003. Les paiements se faisaient en liquide, par des versements sur des comptes irakiens à l'étranger ou par la livraison de biens.

En termes financiers, le réseau irakien semble avoir utilisé trois méthodes pour dissimuler les transferts d'argent, c'est-à-dire à la fois leur destination et leur finalité :

- La première consistait à financer certaines transactions par des paiements en liquidités effectués par les agents des SSI implantés dans les pays des fournisseurs. Les biens ainsi obtenus pouvaient alors être livrés par la voie diplomatique jusqu'à la Jordanie ou la Syrie puis transférés en contrebande en Irak. Le transfert d'argent de ces pays vers l'étranger se faisait par la valise diplomatique pour éviter la détection du mouvement interbancaire[61].
- Deuxième méthode, essentiellement après 1999, le paiement par des sociétés écrans possédant des comptes dans les banques de pays proches (Jordanie, Syrie). Les paiements s'effectuaient par des virements bancaires (lettres de crédits) à la livraison du ou des biens concernés. Les comptes des sociétés écrans étaient alimentés par la banque centrale irakienne via ses avoirs dans les banques nationales des pays servant de plaques tournantes. C'est ainsi développé un réseau de plusieurs dizaines de comptes internationaux, sous des noms de personnes physiques et sous le contrôle financier de la banque centrale, afin de recevoir les fonds provenant des ventes de produits pétroliers illicites et de gérer leur utilisation par les organisations irakiennes intervenant au sein du réseau. A partir de 1996, une partie de l'argent provenant du trafic de produits pétroliers était transférée manuellement en Irak par des délégations de la banque centrale irakienne afin de permettre de payer directement les fournisseurs étrangers par la première méthode.
- Enfin, l'Irak a pratiqué le troc, c'est-à-dire le financement d'acquisition par la distribution de bons de tirage sur la production de pétrole. Ce système semble avoir été utilisé ponctuellement en complément de financement en liquide. Le système des bons de tirage était en revanche plus abondamment utilisé pour corrompre des officiels étrangers, y compris dans le cadre des activités du réseau d'acquisition.

### ➧ Fonctionnement, diffusion et assimilation des biens achetés

Le Comité pour l'Industrialisation Militaire (MIC) était le principal bénéficiaire des activités du réseau d'acquisition irakien.

Le MIC recevait annuellement les demandes de matériels émanant de l'un des 51 établissements sous son contrôle dans le cadre du processus budgétaire, et lançait des appels d'offres vers ses intermédiaires. Les commissions des importations du MIC, sous la direction du département technique, étaient chargées de procéder à la sélection des fournisseurs sur la base des offres reçues, en particulier à l'occasion de la foire annuelle de Bagdad. Outre ses ressources propres, dont la partie illicite était déposée sur des comptes étrangers en Jordanie, en Syrie ou au Liban, le MIC pouvait également puiser, pour honorer ses contrats, dans les fonds de la banque centrale irakienne.

Toutefois, une partie des approvisionnements faisait l'objet d'une coordination avec les SSI, sous la responsabilité du bureau de la Recherche et du développement du MIC.

[61] ISG Final Report, p. 46.

Dans ce cadre, plus informel, des réunions pouvaient être organisées entre les fournisseurs potentiels et les ingénieurs de l'établissement utilisateur[62].

Le réseau d'acquisition irakien a servi à alimenter les programmes, en particulier le programme de missiles, en composants parfois critiques pour leur développement. A titre d'exemple, l'achat de plusieurs centaines de moteurs Volga a répondu efficacement aux besoins de développement du programme Samoud et à la contrainte imposée par la Commission Spéciale[63].

Malgré quelques succès en termes techniques, on peut toutefois s'interroger sur l'efficacité d'ensemble du réseau[64]. En effet, le système mis en place par l'Irak, en multipliant les intermédiaires et les intervenants administratifs, laissait peu de place à l'évaluation technique des offres par les utilisateurs. Tout porte à croire que les affaires entièrement traitées par les SSI ont sans doute conduit à l'acquisition de biens inutiles pour les programmes considérés. La mise en place à partir d'octobre 1999 d'une véritable coordination entre le MIC et les SSI a sans doute permis de corriger en partie cette faiblesse.

Le fonctionnement du système a également été rendu possible par la complicité des gouvernements de certains voisins de l'Irak, bénéficiaires des accords commerciaux et qui ont sciemment facilité les flux générés par les efforts d'acquisition. Ainsi, le recours systématique à de faux documents – certificats d'utilisation finale, déclarations de douanes ou de chargement – et la dissimulation de l'utilisateur final ont été rendus possibles par l'existence de ces liens privilégiés. Cette méthode a permis au réseau irakien d'obtenir auprès de sociétés, participant volontairement ou non, les biens recherchés en contournant les systèmes de contrôle des exportations.

De même la coopération bancaire avec certains de ces États a été essentielle pour faciliter les mouvements d'argent entre l'Irak et ses clients. Cette coopération a impliqué aussi bien les banques centrales de part et d'autre mais également des banques commerciales. Ainsi, la banque irakienne Rafidian, qui possède des branches dans plusieurs pays de la région du Golfe et en Europe, a servi d'intermédiaire entre la banque centrale irakienne et ses homologues ou les banques dont l'Irak était le client[65].

Très structuré et évolutif, le réseau irakien a su utiliser les ressources disponibles, mal contrôlées par les Nations Unies, pour parvenir à alimenter les programmes du pays malgré un embargo sévère. Même si certains aspects de son fonctionnement sont probablement uniques, il n'en reste pas moins que le modèle est sans doute valable pour d'autres réseaux d'acquisition, en particulier ceux reposant sur des fonds acquis illicitement. A titre d'illustration, le réseau nord-coréen doit être assez semblable à celui de l'Irak, en particulier en termes financiers avec l'utilisation de banques relais destinées à la fois à blanchir l'argent issu des divers trafics et à financer les achats. Ainsi, le gel des avoirs nord-coréens déposés à la banque Banco Delta Asia, qui a conduit la Corée du Nord à transférer des fonds vers d'autres comptes en Europe ou en

[62] ISG Final Report, p. 68.

[63] En 1996, la Commission avait interdit à l'Irak d'utiliser les moteurs de son parc de SA-2 pour le développement du Samoud.

[64] A titre d'exemple, l'achat en 1995 de gyros de missiles balistiques lancés des sous-marins ; ces composants étant inutilisables dans le cadre du programme de missiles irakiens.

[65] La banque Rafidian possédait des succursales au Liban, en Jordanie, en Égypte, au Koweït et même au Royaume Uni.

Asie[66], semble avoir touché autant le réseau d'acquisition nord-coréen que certains des trafics illégaux de Pyongyang. L'utilisation systématique des voies diplomatiques pour les mouvements d'argent liquide semble également faire partie de l'arsenal des moyens employés par la Corée du Nord pour alimenter son réseau d'acquisition.

## *1.2 – Modélisation des réseaux de prolifération*

### *1.2.1 – Les réseaux de fournisseurs*

➧ **Analyse fonctionnelle**

Pour fonctionner, un réseau de fournisseur doit être en mesure de proposer à ses clients le produit (ou les produits) le plus adapté à leur besoin, à un coût correspondant à leur budget mais également être capable de le livrer de façon discrète. Il s'agit là des capacités clefs d'un réseau de fournisseurs, auxquelles il convient d'ajouter une série de prestations optionnelles comme, par exemple, la mise en place d'une assistance technique sur place ou en amont pour la définition du besoin[67].

Ainsi, il paraît possible de dégager les fonctions essentielles que doit assurer un réseau de fournisseurs :

- Technique : c'est-à-dire la capacité de proposer une offre correspondant au besoin du client. L'existence de cette fonction constitue la condition nécessaire pour que le réseau existe, dans la mesure où il est capable de proposer un produit ou un service. Ce dernier peut être primaire (un composant particulier) ou élaboré (une offre complète, des connaissances ou savoir-faire). La fonction technique peut être assurée par le réseau lui-même, sous-traitée à des fournisseurs – volontaires ou non –, ou encore être partagée entre des fournisseurs extérieurs et une partie du réseau.
- Logistique : à la fois la gestion de la production ou de l'acquisition du bien concerné et son acheminement vers le client. Pour certaines affaires, l'acheminement peut n'être assuré qu'en partie par le réseau lui-même et pris en charge pour partie par le client[68]. De même, la production peut être sous-traitée à des sociétés travaillant au profit du réseau, comme ce fût le cas de SCOPE. En tout état de cause, la coordination avec le client et la gestion des flux en interne constituent l'une fonction clef pour le réseau.

[66] « N. Korea now channelling overseas cash via Austria after U.S. sanctions on Macau bank », *East Asia Intel*, 21 décembre 2005.

[67] C'est le « plus » du réseau Khan.

[68] En particulier, si ce dernier dirige un réseau d'acquisition propre. Pour prendre un exemple, dans le cas de la proposition de Khan aux Irakiens, ces derniers auraient sans doute souhaité avoir le contrôle d'une partie de l'acheminement.

➡ Financière : il s'agit de la capacité de gestion des flux financiers, à la fois au sein du réseau pour payer les intermédiaires et fournisseurs et avec l'extérieur. Le réseau doit être à même de recevoir les paiements des transactions et de les distribuer aux divers intervenants, tout en camouflant les opérations. Cela signifie qu'il est capable de blanchir l'argent reçu de ses clients, mais également d'utiliser ses fonds pour acquérir des biens au profit de ces derniers.

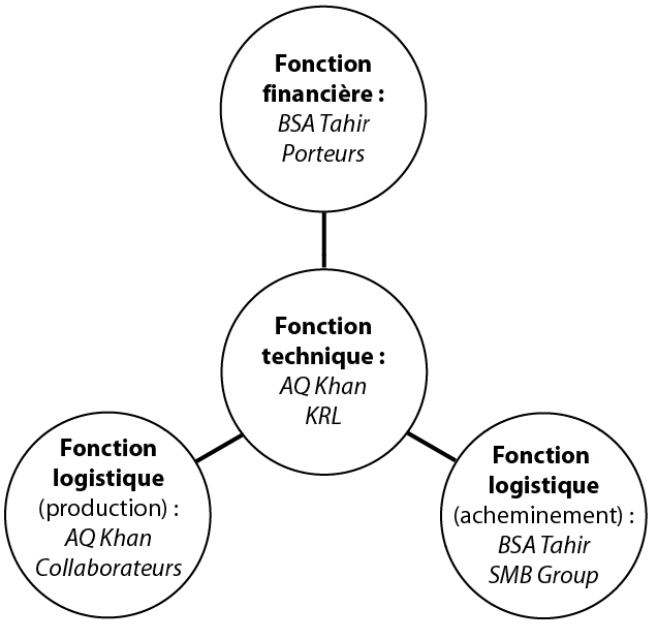
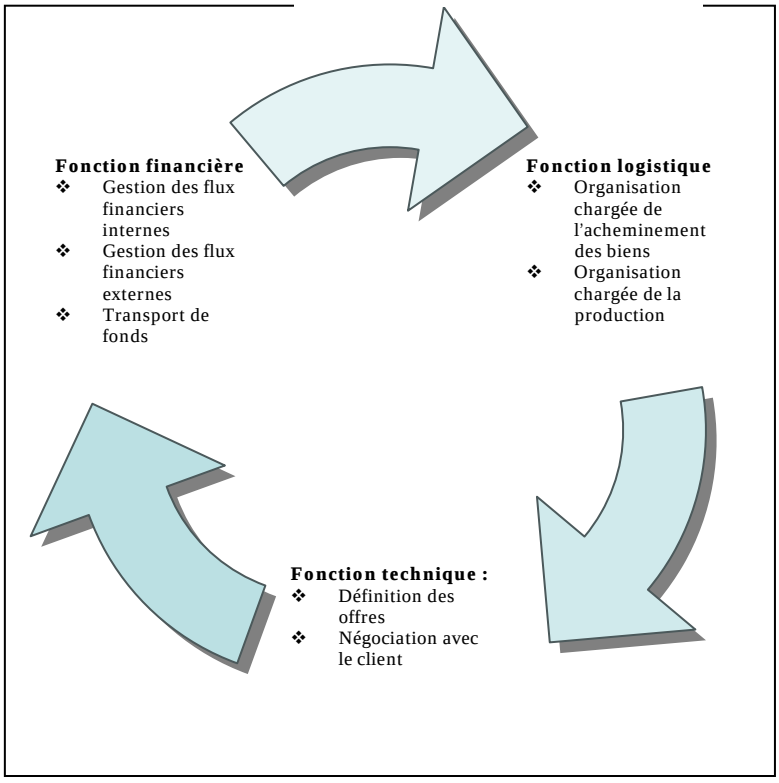


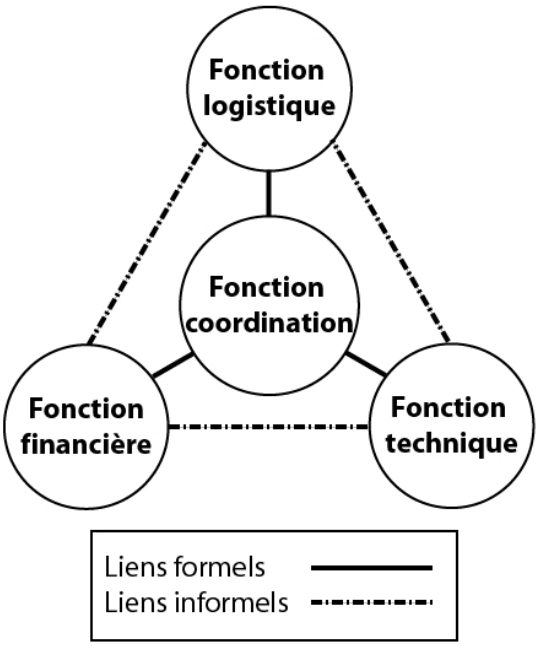

Fig. 1 **: distribution des fonctions assurées par le réseau Khan**

Fig. 2 : Distribution des fonctions dans un réseau étatique



Les interactions entre ces fonctions déterminent la structure même du réseau. Si l'on reprend le cas du réseau A. Q. Khan, certaines fonctions sont assurées par une seule et même personne. Ainsi, la gestion des acheminements et des flux financiers revient à BSA Tahir, celle des aspects techniques et de production à A. Q. Khan et à certains intermédiaires ou collaborateurs. Toutefois, dans ce cas de figure, une seule personne est chargée de coordonner les fonctions clefs. Si cet aspect centralisé confère une bonne efficacité à l'organisation à partir du moment où la personne clef est compétente, elle la rend également vulnérable à sa disparition. Cette faiblesse peut être compensée si l'échelon central possède une ou plusieurs redondances, c'est-à-dire des personnes ou une organisation capables d'assurer la fonction de coordination en cas de défaillance.

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




Les réseaux davantage structurés autour d'organisations que de personnes apparaissent moins fragiles[69]. Du fait de leur caractère étatique, ils profitent également de moyens supplémentaires en termes d'acheminement et d'opérations financières. En particulier, ils peuvent transporter des biens avec les moyens nationaux ou bénéficier des avantages diplomatiques. En revanche, le poids structurel imposé par l'implication d'organisations est de nature à nuire à l'efficacité d'ensemble. La coordination entre les fonctions techniques, logistiques et financières peut donc être source de difficultés pour le réseau du fait, entre autres, des compétitions ou même de l'absence de coopérations entre les organisations impliquées. Toutefois, cette difficulté paraît moins cruciale pour le fonctionnement d'un réseau de fournisseurs qu'elle ne peut l'être pour l'acquisition.

Deux modèles de base sont donc envisageables pour les réseaux de fournisseurs, qui correspondent à des réalités différentes :

- Un modèle en étoile, qui correspond *a priori* à un réseau privé ou semi-privé (type Khan, fig. 1).
- Un modèle cyclique, qui correspond *a priori* à un réseau étatique (de type nord-coréen, fig. 2).

Des combinaisons des deux modèles sont envisageables, qui correspondraient à la structure du réseau Khan entre 1992 et 1999, et dans lequel sont impliquées des organisations de l'État concerné avec un contrôle central exercé par un individu. L'existence d'organisations possédant une structure plus informelle, dans laquelle chaque centre est lié aux autres mérite d'être évoquée[70]. D'un point de vue fonctionnel, un tel réseau paraît relativement complexe à gérer. Il est toutefois envisageable dans un scénario de dégradation de réseaux cycliques ou en étoile dans lesquels les intervenants

[69] C'est, par exemple, le cas du réseau nord-coréen de fourniture de technologies de missiles.

[70] Alexander H. Montgomery, « Ringing in Proliferation », *International Security*, op. cit., p. 170.

auraient cessé de se coordonner à un niveau global pour tisser des liens informels entre eux (fig.3). Une telle configuration rend le réseau moins vulnérable à la disparition de l'instance de coordination ou de l'un des pôles fonctionnels que dans les cas de base décrits plus haut.

➧ **Organisation d'ensemble : contournement des réglementations, opérations financières et logistiques, points forts et faibles**

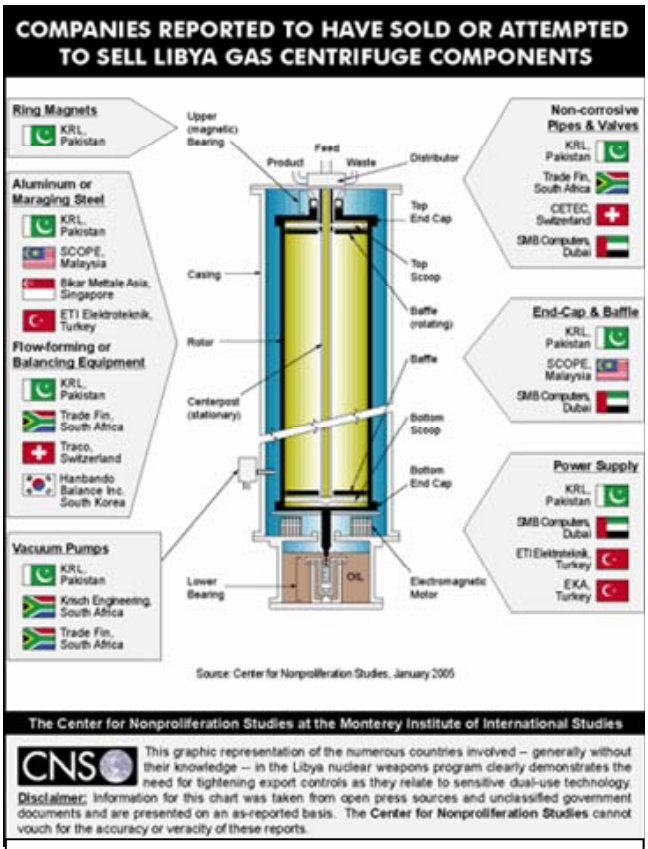



Schéma indiquant l'origine des diverses pièces constitutives de l'offre du réseau A. Q. Khan à la Libye (source : Center for Non Proliferation Studies)

Quelle que soit sa structure fonctionnelle, la mission d'un réseau de fournisseur est de livrer à ses clients un produit conforme à leurs besoins. Pour ce faire, il doit être à même, dans certains cas, d'acquérir au profit de son client certains biens et de les acheminer, éventuellement en complément de sa propre offre. Ainsi, le réseau Khan achetait au profit de ses clients des biens auprès de diverses entreprises européennes, asiatiques ou encore sud-africaines.

Pour parvenir à conduire ce type d'opération, le réseau doit être en mesure de contacter des entreprises étrangères et de s'assurer que l'exportation des biens n'est pas détectée par les autorités nationales. En termes d'organisation, le réseau devra donc rechercher et utiliser des intermédiaires ayant une bonne connaissance du tissu industriel local et étant au fait des faiblesses des systèmes nationaux de contrôle des exportations. Il est également impératif que le réseau possède des sociétés écrans qui seront les acheteurs officiels et devront assurer le transit des biens vers leur véritable destinataire.

Ces sociétés écrans jouent également le rôle de transitaires pour les biens qui sont acquis par les intermédiaires et doivent en assurer l'acheminement. Il s'agit donc de choisir leur implantation physique de façon à ce qu'elles assurent la réexportation, sans ou avec un minimum de contrôle sur la transition des biens acquis.

Pour dissimuler leur destination, dans le cas le plus contraignant c'est-à-dire celui d'un pays possédant un système de contrôle efficace, les intermédiaires et sociétés écran devront mettre en place une série de mesures :

- Faux documents : en particulier, des faux certificats de destination finale voire des certificats de non-réexportation falsifiés, quand ils sont exigés pour obtenir l'autorisation d'exportation depuis le pays concerné. Dans certains cas, ces documents doivent être contresignés par les autorités nationales du pays accueillant la société

écran[71]. Des complicités au niveau administratif sont alors nécessaires. Ainsi, dans le cas de la fourniture de cellules de missiles de croisière AS-15/Kh-55 par l'Ukraine à l'Iran et à la Chine via la Russie, un ou plusieurs fonctionnaires de Rosoboronexport avaient été amenés à signer des certificats d'utilisateur final, permettant l'obtention d'une autorisation ukrainienne. L'utilisation de faux manifestes de cargaison, afin de dissimuler la nature du produit, constitue enfin une solution pour échapper aux efforts des douaniers et des services de renseignement.

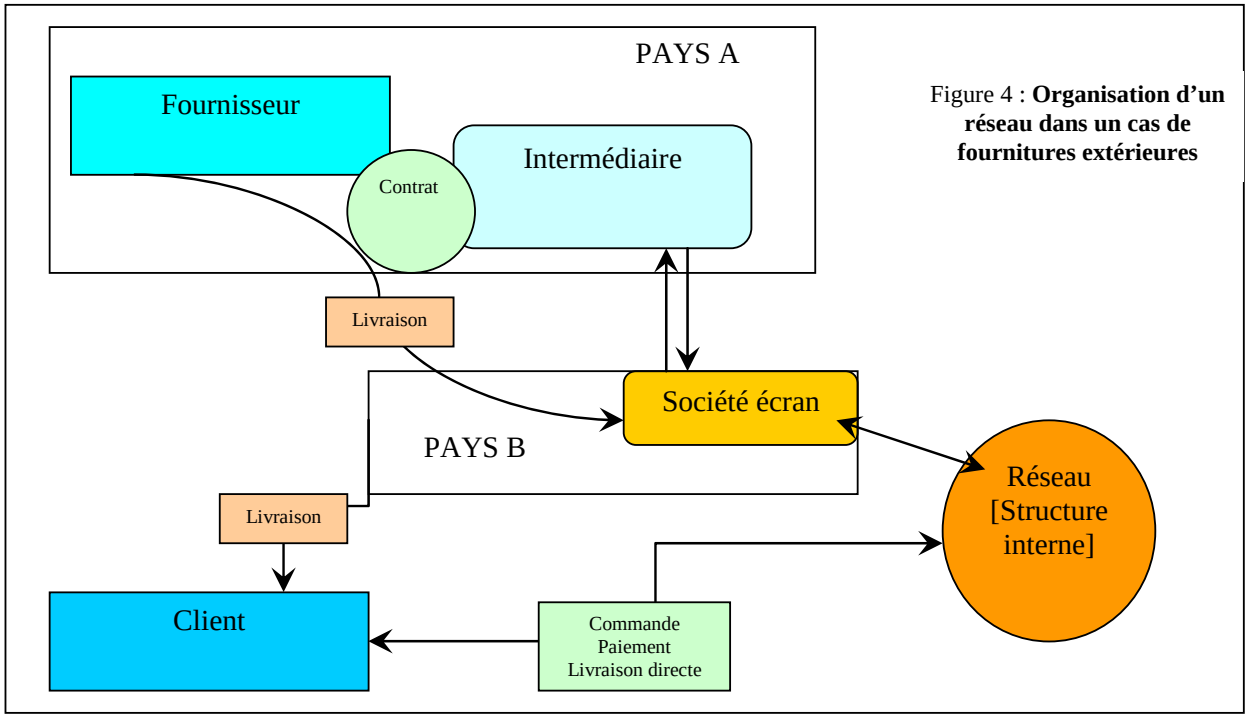



Figure 4 : **Organisation d'un réseau dans un cas de fournitures extérieures**

➥ Choix des produits, des fournisseurs et des transporteurs : pour contourner les systèmes existants de contrôle des exportations, la partie extérieure du réseau (intermédiaires et sociétés écran) doit autant que possible choisir des biens fortement duaux ou qui ne sont pas considérés comme sensibles au regard de la destination déclarée. Il est aussi possible de sélectionner des composants élémentaires plutôt que des sous-ensembles complets dont l'utilisation est plus simple à établir. A titre d'exemple, dans le cas libyen, les éléments fabriqués par SCOPE, utiles en matière de prospection pétrolière, pouvaient légitimement être destinés à une société émirienne. En d'autres termes, le réseau doit pouvoir couvrir son activité par des opérations légitimes, en exploitant la diversité des fournisseurs et l'implantation des sociétés écrans. Enfin, c'est à lui que revient le choix des transporteurs, dans les cas où l'acquéreur ne peut pas utiliser des moyens propres.

Dans le cas où le réseau ne pratique pas d'acquisitions de matériel à l'étranger au profit de ses clients, il peut réduire sa structure externe au minimum. Il doit alors posséder ses propres moyens d'acheminements (supposés sûrs), pour les biens comme éventuellement pour l'assistance technique.

[71] C'est le cas pour les matériels sensibles – militaires comme à double usage – exportés depuis les États-Unis. Certains pays européens commencent à exiger ce type de visa pour les matériels à double usage ou militaires.

Les mouvements de capitaux ou d'argent sont quant à eux détectables dans la plupart des cas, même s'il s'agit de virements bancaires directs entre banques nationales[72]. Pour les réseaux de fournisseurs, la principale difficulté tient d'ailleurs au volume des opérations bancaires réalisées. Ainsi, un réseau utilisant des intervenants extérieurs pour une partie de ses activités devrait réaliser un nombre important d'opérations financières, contrairement à une organisation offrant sa seule production. Plusieurs choix opérationnels peuvent se présenter pour gérer ces flux :

- Réaliser le plus possible d'opérations en numéraire : l'utilisation de devises pose toutefois le problème de leur réintroduction sur le marché, c'est-à-dire de leur blanchiment. Certains pays ont introduit des règles limitant le montant des paiements en liquide[73], ce qui doit empêcher les réseaux de procéder à des règlements numéraires d'éventuels fournisseurs[74]. Dès lors, au vu de la taille des flux financiers générés (en millions de dollars[75]), ce marché ne peut s'organiser uniquement par des transferts en devises. En revanche, la rémunération en liquide d'une partie du réseau, en particulier les intermédiaires ou les sociétés complices, paraît envisageable.
- L'utilisation d'un réseau de banques et d'institutions financières : il s'agit pour le réseau de placer une partie de ses ressources financières dans plusieurs banques ou institutions financières qui se chargeront de recevoir les paiements et de gérer les flux financiers destinés à alimenter les divers acteurs. Ainsi, Pyongyang semble avoir réparti les revenus générés par ses activités illicites dans plusieurs banques asiatiques, européennes et américaines[76]. Il est également possible, pour certains réseaux, d'implanter à l'étranger des institutions financières sous leur contrôle dont le rôle exclusif est d'administrer leurs avoirs, payer les fournisseurs et recevoir les paiements des clients. Une telle solution – semblable à celle mise en place par l'Irak à travers la banque Rafidian – présente l'intérêt de limiter le risque de gel des avoirs et de permettre la réalisation d'opérations illicites sans risquer la détection par les services de contrôle financier.

[72] En effet, l'automatisation des virements bancaires a conduit à la mise en place d'un réseau sécurisé international activé par la société SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) qui connecte 7 800 institutions financières dans 202 pays. Centralisée en Belgique, SWIFT a ouvert une "porte dérobée (*backdoor*)" à la CIA pour contrôler les flux après le 11 septembre 2001.

[73] « Le blanchiment progresse en dépit d'une vigilance accrue », *Le Monde*, 23 mai 2006.

[74] Ceux qui ne sont pas complices du réseau.

[75] Les bénéfices qui auraient été générés par le réseau Khan s'élèveraient à quelques centaines de millions de dollars.

[76] « U.S. insists sanctions on N. Korea are having worldwide 'ripple effect' », *East Asia Intel*, April 12, 2006.

**BLANCHIMENT ET « NOIRCISSEMENT » D'ARGENT DANS LA PROLIFERATION**

## 1. Blanchiment d'argent

Définition[77]

Le blanchiment d'argent est un élément des techniques de la criminalité financière. C'est l'action de dissimuler la provenance d'argent acquis de manière illégale (dans notre cas le trafic de produits proliférants interdits à l'exportation) afin de le réinvestir dans des activités légales. C'est une étape importante, car sans le blanchiment, ces entreprises ne pourraient pas avoir des réseaux de prolifération comme clients (il leur faut faire passer le fruit de ces ventes illégales dans leurs comptes) et ne pourraient utiliser de façon massive ces revenus sans être repérées.

On distingue généralement plusieurs étapes dans le processus de blanchiment : le **placement** des sommes en produits financiers, **l'empilage** des intermédiaires pour perdre la trace de l'origine et enfin la **réintégration** des fonds dans l'économie légale.

Méthodes de blanchiment en général et celles utilisées dans la prolifération

- « **Schtroumpfage »** : dépôt en banque de petites sommes en espèces par plusieurs personnes.
- **Complicité bancaire** (d'une banque ou d'un employé) : par exemple les Rasheed Bank et Rafidian/Rafidain Bank pour l'Irak[78], la Banque Delta et la succursale de la Banque (étatique) de Chine populaire à Macao pour la Corée du Nord.
- **Achat de biens au comptant** et en espèces : mais ceci n'est pas possible si l'État qui se dote d'armes interdites veut une relation durable avec ses fournisseurs et ne veut pas être soupçonné.
- **Transfert électronique de fonds** : si la surveillance par la CIA et le département du Trésor du réseau interbancaire SWIFT se poursuit, cette méthode laissant des traces est trop risquée[79].
- **Amalgamation de fonds dans des entreprises honnêtes** : cette méthode est trop lente pour des pays proliférants qui ont des besoins rapides.

S'il est possible de lutter contre des réseaux étatiques d'approvisionnement en produits « sensibles » (matière fissile, composant figurant sur la liste du Comité de Zangger ou du MTCR), il est en revanche beaucoup plus difficile de lutter contre des opérations *a priori* légales (ventes de sous-ensembles, de pièces détachées dont l'utilisation finale n'est pas connue) mais qui s'avèrent être des trafics de biens à double usage.

## 2. « Noircissement » d'argent[80]

Le noircissement d'argent est l'inverse du blanchiment d'argent.

Si la préoccupation principale des fournisseurs payés par des réseaux de prolifération est de réinjecter des revenus illicites dans l'économie officielle, le souci d'un État qui souhaiterait développer des activités illicites (achats de pièces interdites à l'importation, corruption) est, à l'inverse, de générer des fonds occultes et de l'argent noir en liquide à partir d'argent légalement acquis.

[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

[80] http://fr.wikipedia.org/wiki/Noircissement_d%27argent

L'affaire « Pétrole contre nourriture » fournit un florilège des techniques de noircissement utilisées par l'Irak : des jeux de commissions, portage par des intermédiaires (fonctionnaires d'ambassades) lors d'opérations d'achat…[81]

**Typologie des problématiques de chaque pays :**

- **Irak, Iran, Libye** (pays exportateurs de pétrole disposant de devises fortes) possédant déjà de l'argent « propre ». Pour ces pays, la question du blanchiment ne se pose pas puisqu'ils disposent déjà d'argent propre (les revenus du pétrole). Ils doivent « noircir » une partie de cet argent qui leur sert à acheter des biens sur le marché mondial ou dans les pays occidentaux pour masquer l'utilisateur et l'utilisation finale. Pour les achats qu'ils effectuent à des pays voyous (Khan Research Laboratory au Pakistan, Corée du Nord…) il n'y a pas besoin de noircir l'argent
- **Corée du Nord** et autres pays ne disposant pas de devises fortes. L'économie nord-coréenne étant exsangue et ne survivant que sous perfusion de l'aide internationale (sud-coréenne, chinoise et du programme alimentaire mondial), le régime de Pyongyang a besoin, avant de pouvoir acheter des importations, d'acquérir ces devises. Elle l'a fait par le passé en diffusant des faux billets de $100 et en vendant des contrefaçons : Viagra, cigarettes et amphétamines en collaboration avec des gangsters chinois[82].
- Les problèmes du **Pakistan** sont probablement les mêmes : pour pouvoir acquérir des technologies qu'il n'a pas (missiles) ou pour que Khan Research Laboratory rentabilise ses usines d'enrichissement, le Pakistan semble être prêt échanger des technologies par le troc (avec la Corée du Nord) ou en les achetant (?).
- Pour les **réseaux semi-privés sub et trans-étatiques** (type Khan) et sous-réseaux, le profit étant l'une des principales motivations, tout acheteur de leur technologie est acceptable, qu'il soit honnête ou malhonnête.
- Concernant les terroristes, plusieurs spécificités rendent leur tâche plus difficile : s'ils n'ont de pays « sanctuaires » (comme l'Iran), il leur est difficile de se faire livrer des missiles ou de matériaux radioactifs. De plus, si le destinataire final est connu, de nombreux fournisseurs pourront hésiter. Au contraire, l'idéologie peut les pousser à prendre plus de risques et leur faciliter l'obtention de biens par des complices partageant les mêmes croyances.
- Individus seuls :
  Ex : Gotthard Lerch[83]
- Les pays « à risque » pouvant exporter illégalement des technologies proliférantes. Outre le Pakistan et la Corée du Nord déjà évoqués, la **Russie** et **la Chine** peuvent inquiéter.

  **Russie** : peu d'affaires (de trafics de matières radioactives) découvertes malgré les possibilités, la réputation de la Russie et les craintes (fantasmées ?).

[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

[83] http://www.newyorker.com/online/content/?060807on_onlineonly

Pour un réseau de fournisseur, la situation idéale finalement serait d'être en mesure de fournir les produits recherchés par ses clients sans avoir à utiliser des intermédiaires et des fournisseurs extérieurs. Il exerce alors un contrôle presque total sur l'ensemble des flux générés par son trafic, et limite les risques de détection et de démantèlement. Les exemples connus de réseaux de fournisseurs (Corée du Nord, Khan) ne correspondent toutefois pas à ce modèle. Deux explications paraissent pouvoir être données à cet état de fait :

- La nature privée de certains réseaux c'est le cas de celui de Khan après 1999 qui les oblige à acquérir certains biens à l'étranger pour répondre à la demande de leur client ; la spécificité de ces réseaux étant en outre de proposer une offre complète (des technologies au cycle de production). Dans la mesure où ils ne sont pas forcément à même de produire en interne tous les éléments nécessaires, l'acquisition externe (sous forme de sous-traitance) s'impose.
- La nature duale de certains réseaux : les réseaux de fournisseurs sont souvent également des réseaux d'acquisition mis en place pour répondre à des besoins nationaux[84]. Les structures existantes pour les activités d'acquisition gèrent également l'activité d'export. Elles sont donc amenées à générer des flux plus importants et à s'appuyer sur des réseaux internationaux plus étendus que si elles ne géraient que les activités export.

### ➧ Détermination de critères applicables pour juger des vulnérabilités d'un réseau de fournisseur

Pour être efficace et pérenne un réseau de fournisseur devrait rechercher trois caractéristiques essentielles :

1. Discrétion : en particulier, échapper à la détection par les organisations chargées de suivre les mouvements suspects de biens et de capitaux : douanes, services de renseignement, polices.
2. Efficacité et "abordabilité" : à la fois être capable de répondre au besoin des clients[85] à des coûts relativement accessibles/abordables pour eux tout en laissant l'opération rentable pour le fournisseur.
3. Résilience : le réseau doit pouvoir continuer à fonctionner si une partie de ses moyens lui sont enlevés ou ne sont plus disponibles.

Pour juger de la vulnérabilité d'un réseau de fournisseur, c'est-à-dire de la possibilité de le neutraliser définitivement ou durablement, il convient de déterminer quelles sont ses conditions minimales de fonctionnement. Il paraît donc judicieux de dégager une série de critères élémentaires permettant de caractériser l'organisation[86].

Le premier est **la taille et l'étendue du réseau** : le nombre de personnes, d'organisations et d'entreprises impliquées dans le réseau. Les plus gros réseaux présentent l'intérêt

[84] C'est le cas de Khan avant 1999 et de la Corée du Nord.

[85] Ce qui implique de connaître les clients, de les contacter et de comprendre leur besoin.

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

de faciliter une gamme d'acquisitions plus importante, ce qui accroît leur efficacité. En revanche, les plus petits réseaux sont moins détectables et leurs opérations plus discrètes car moins nombreuses. Toutefois, ils sont plus vulnérables à des actions de neutralisation dans la mesure où il existe peu voire pas de redondance en leur sein.

Deuxième critère applicable, **la concentration fonctionnelle du réseau** : le nombre de fonctions qui sont tenues par une seule ou quelques cellules au sein du réseau. Ainsi, dans le réseau Khan, dans l'état de nos connaissances, certaines fonctions étaient assurées par quelques personnes. C'est le cas en particulier de la coordination du réseau et de la fonction technique, dont *a priori* seule une poignée de personnes auraient été responsables[87]. BSA Tahir, par exemple, intervient comme coordinateur des fonctions logistiques et financières. Cette concentration fonctionnelle présente un risque pour la survie de l'organisation. En revanche, elle peut présenter un intérêt en termes d'efficacité puisqu'elle évite une dilution des responsabilités qui peut entraîner des difficultés de coordination.

Le dernier critère est celui de la **compétence technique du réseau**. Il mesure la capacité de l'organisation à proposer une offre techniquement viable et à assurer la livraison du produit à son client. En première analyse, les réseaux les plus compétents semblent être ou avoir été adossés à une compétence technique nationale (cas nord-coréen et pakistanais). D'autres réseaux, comme celui qui a transféré en 2000 une dizaine de cellules d'AS-15 ukrainiennes à l'Iran et à la Chine, paraissent ne pas avoir une connaissance importante du produit mais être capables d'organiser efficacement son exportation vers les clients.

Sur la base de ces critères, il paraît possible de dresser un bilan de la vulnérabilité de nos modèles de réseaux. Les organisations privées se caractérisent selon toute vraisemblance par une forte concentration fonctionnelle, même s'ils peuvent être étendus. A la lumière des exemples connus, il apparaît que leur compétence technique n'est pas homogène, mais qu'ils sont capables d'assurer assez efficacement la gestion des flux générés. Quant aux réseaux étatiques, tout porte à croire qu'ils sont relativement étendus, mais ne présentent pas de concentration fonctionnelle notable. Leur compétence technique dépend directement de celle des États qu'ils représentent.

| | | **Étendue** | **Concentration fonctionnelle** | **Compétence technique** | **Vulnérabilité** |
|---|---|---|---|---|---|
| **Réseaux privés ou semi-privés** | Réseaux centralisés | Grande | Moyenne à grande | meilleure | Faible car redondances |
| | Réseaux informels | Petite | Élevée | Faible à bonne | Forte |
| **Réseaux étatiques** | | Grande | Faible | Variable | Faible |

**Tableau 1 : Détermination des critères pour les modèles de réseaux**

[87] Pour la partie technique, Khan et peut être certains de ses proches comme Anwar Ali. Voir, Leonard Spector & Haider Nizamani, « New Head of Pakistan Atomic Energy Commission Apparently Tied to 1980s Nuclear Smuggling », *WMD insights*, May 4, 2006.

### *1.2.2 –Les réseaux d'acquisition*

➧ **Analyse fonctionnelle**

Structurés autour de l'objectif d'obtenir à l'étranger des composants ou des savoir-faire nécessaires aux programmes nationaux d'armes de destruction massive, les réseaux d'acquisition regroupent *a priori* deux organisations fonctionnelles élémentaires :

- La première, chargée de la spécification du besoin, sert d'intermédiaire entre l'utilisateur du produit et l'organisation chargée de son achat. Il s'agit pour cette partie du réseau de définir les composants, les systèmes ou les technologies qui répondent le mieux au besoin exprimé par le bénéficiaire. Par exemple, dans le cas irakien, le Comité de l'Industrialisation Militaire (MIC) était chargé de cette fonction, sur la base des demandes effectuées par les directeurs des centres de production ou de recherche.
- L'organisation chargée des achats/acquisitions doit à la fois trouver les fournisseurs susceptibles de répondre aux besoins exprimés, contractualiser directement avec ces derniers ou avec des intermédiaires chargés de les approcher et contrôler les flux financiers nécessaires pour payer les fournisseurs et les intermédiaires. En termes fonctionnels, cette organisation présente de nombreuses similitudes avec un réseau de fournisseur, mais s'en écarte par quelques aspects. D'un point de vue logistique, le réseau peut se limiter au transport du matériel entre des sociétés écrans établies à l'étranger et l'utilisateur final, le reste des opérations étant pris en compte par les intermédiaires ou les fournisseurs. Cette fonction n'apparaît toutefois pas essentielle pour permettre son fonctionnement[88]. En revanche, la fonction financière est prédominante, puisqu'il est nécessaire de gérer des flux au sein du réseau lui-même, y compris des sociétés écrans lui appartenant, mais également avec les intermédiaires éventuels et les fournisseurs. A ces différences près, on peut *in fine* considérer que les modèles développés pour les réseaux de fournisseurs sont applicables à ces organisations.

[88] Le cas irakien montre toutefois qu'un réseau d'acquisition peut prendre à son compte une grande partie de l'acheminement.

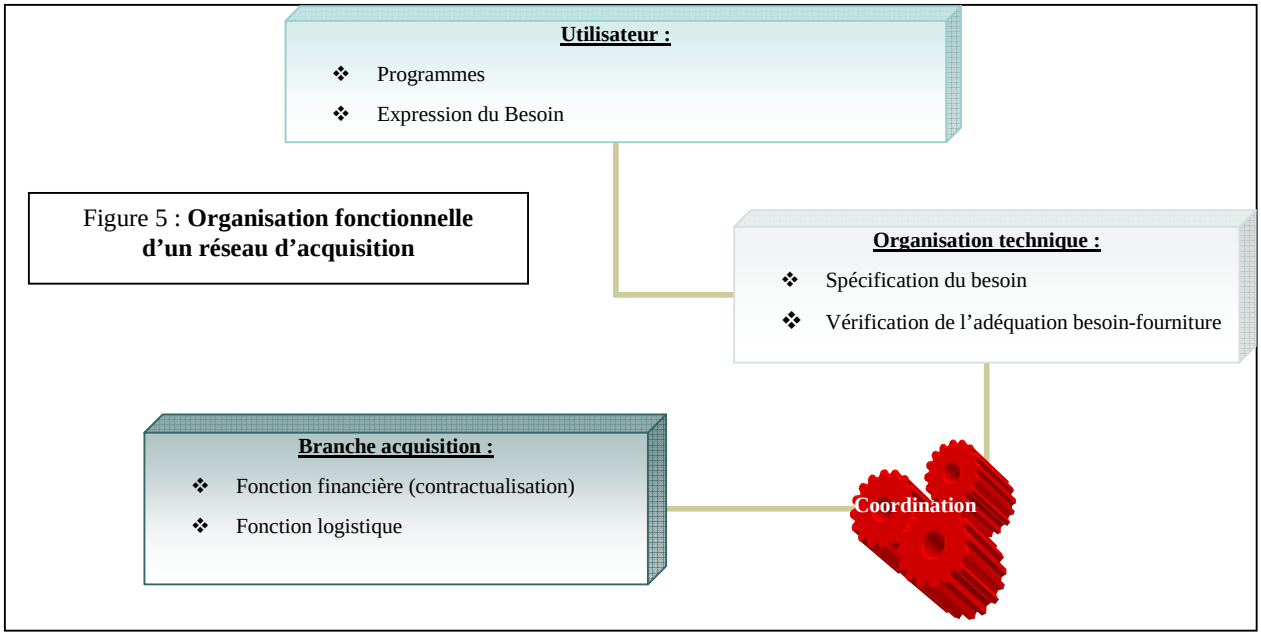



Figure 5 : **Organisation fonctionnelle d'un réseau d'acquisition**

Ce qui fait la spécificité des réseaux d'acquisition est leur capacité à coordonner ces deux branches de leur activité. Comme nous l'avons vu avec l'exemple irakien, la coexistence de deux organisations concurrentes chargées de l'acquisition, la première dépendant du MIC et la seconde des services secrets, a longtemps nui à l'efficacité du réseau. A partir de 1997, la coordination de ces systèmes a permis au MIC de profiter des services uniques offerts par les services secrets mais également d'améliorer la capacité de ces derniers à répondre à certains besoins exprimés par les centres techniques. Cette fonction de coordination ne se limite pas à trouver le meilleur moyen de répondre au besoin exprimé par l'utilisateur, elle doit également permettre à ce dernier de dialoguer indirectement avec les fournisseurs afin d'obtenir le produit le plus adapté à son besoin[89]. Il peut s'agir d'ailleurs de mettre directement en contact l'utilisateur et le fournisseur, par exemple dans le cadre de formation ou de transferts de technologie.

Dans la mesure où ces réseaux sont essentiellement de nature étatique, la branche d'acquisition a une structure de type centralisée conformément au modèle présenté précédemment. La fonction de coordination peut se trouver sous sa responsabilité ou être partagée avec la branche technique. Ainsi, dans le cas irakien, il existait une instance de coordination entre la branche acquisition du MIC et les services secrets.

En tout état de cause, tout laisse à croire qu'il s'agit là d'organisations pérennes et relativement structurées. Même si, en théorie, ces réseaux sont parfois considérés comme informels et donc capables de s'adapter rapidement[90], le fait qu'ils s'appuient en réalité sur un environnement composé d'intervenants extérieurs leur donne une stabilité dans le temps.

[89] Cette notion de dialogue est par exemple présente dans l'organisation de discussions techniques entre les ingénieurs du MIC et des fournisseurs conduites par l'intermédiaire des agents présents à l'étranger.

[90] Alexander H. Montgomery, « Ringing in Proliferation », *International Security*, op. cit.

### ➧ Organisation des réseaux d'acquisition

La vulnérabilité des réseaux d'acquisition tient donc surtout aux intervenants extérieurs dont ils dépendent pour fonctionner, c'est-à-dire le tryptique sociétés écrans–banques–intermédiaires.

Il est possible de séparer cet ensemble en deux principaux groupes :

- Entreprises appartenant au réseau : établissements financiers ou sociétés que le réseau établit à l'étranger pour faciliter ses opérations d'acquisition. Rémunérées par la branche acquisition, elles remplissent des fonctions de représentants directs (mais dissimulés) du réseau.
- Entreprises n'appartenant pas au réseau : de façon générale, une série d'entreprises participant de façon occasionnelle ou involontaire aux activités d'acquisition comme des établissements financiers échangeant des flux avec des banques contrôlées, des intermédiaires agissant pour le compte d'une société écran ou encore des fournisseurs. Il peut d'ailleurs s'agir de réseaux de fournisseurs, comme par exemple celui d'A. Q. Khan ou le réseau nord-coréen.

Pour faciliter son fonctionnement, la structure d'acquisition peut s'appuyer sur la présence sur place d'agents sous son contrôle direct : membres des services secrets – à l'instar de l'Irak – ou personnes de la branche technique envoyées ponctuellement pour la négociation de telle ou telle affaire. Ainsi, dans le cas irakien, une fois les premiers contacts pris avec un fournisseur ou un intermédiaire, les membres du MIC étaient parfois dépêchés sur place pour revoir les clauses techniques et/ou financières du contrat. Ces agents peuvent également être envoyés auprès d'un fournisseur pour recueillir une technologie ou un savoir-faire de façon illicite ou non[91]. Ils peuvent également servir de courrier pour certaines affaires en transportant biens ou devises.

Toutefois, leur rôle essentiel est de servir de points de contact permanents avec les entreprises extérieures au réseau, d'établir dans les pays cibles des structures légales permanentes ou occasionnelles – typiquement des sociétés écrans – permettant de conduire certaines affaires selon les besoins et de gérer les activités internationales, entre autres financières, du réseau. Pour améliorer la sécurité des opérations, ces acheteurs peuvent utiliser deux méthodes particulières[92] :

- Contacter plusieurs fournisseurs potentiels pour un même bien : le MIC irakien a beaucoup pratiqué cette méthode consistant à appeler plusieurs offres, parfois publiquement, pour répondre à un besoin spécifique[93]. Outre les intérêts économiques et techniques[94] d'une telle démarche, elle permet surtout de réduire le risque de ne dépendre que d'une seule source d'approvisionnement. Dans le cas d'un programme établi, il est souvent essentiel de bénéficier sur une durée assez longue de

[91] Ce fut le cas par exemple d'A. Q. Khan dans les années 1970 en Europe.

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

[93] Voir également le cas de la société indienne *Indian Rare Earths Ltd.*, associée au projet d'enrichissement de Delhi. 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] Notamment la possibilité d'obtenir des données techniques sur le matériel et ainsi d'affiner la définition du besoin, voire d'obtenir des modifications sur des composants.

fournisseurs capables de vendre plusieurs fois des composants spécifiques pour des raisons de sûreté d'approvisionnement. Par exemple, la production d'un missile donné peut dépendre de la capacité d'acquérir périodiquement des composants critiques dont la fabrication n'est pas maîtrisée dans le pays. A l'inverse lorsqu'il s'agit d'une opération unique, ce procédé permet de minimiser les pertes en cas de découverte par les autorités du pays concerné.

- Dissimuler un composant critique dans une liste de composants banals : cette technique peut avoir deux finalités. Légitimer un appel d'offres émanant d'une société établie dans un secteur donné vers un fournisseur en dissimulant un bien convoité par le réseau parmi des éléments dont elle pourrait effectivement avoir l'utilité pour ses activités[95]. Rendre plus difficile la tâche des autorités nationales de contrôle en accroissant le volume des demandes qui doivent être traitées par elles.

La multiplication des intervenants semble également constituer une tendance lourde en matière d'organisation des réseaux d'acquisition. Ainsi, une première société d'intermédiation répondant à un appel d'offres donné, émanant d'une société écran, pourra elle-même faire appel à plusieurs autres courtiers, qui peuvent d'ailleurs être situés dans des pays différents. Ces intermédiaires contribuent à accroître le nombre d'opérations logistiques et bancaires associées à l'acquisition et au transport d'un bien donné, rendant encore plus difficile l'identification du destinataire final et la détection d'une opération donnée. Ce d'autant que, comme nous l'avons vu précédemment, ces intermédiaires déguiseront le plus souvent, quand ils les connaissent, la nature de l'utilisation finale ou même l'identité du destinataire.

La nature même des entreprises d'intermédiation constitue un atout supplémentaire pour l'efficacité des opérations d'un réseau d'acquisition. S'agissant pour l'essentiel d'individus, appuyés sur des structures commerciales légères[96], ils jouissent d'une forte mobilité (financière et géographique) qui leur permet d'opérer depuis n'importe quel pays. De ce fait, ils peuvent s'affranchir en partie des contrôles qui leur sont imposés en s'installant dans un État ne disposant pas de législation régissant leurs activités. Pour prendre un exemple, un courtier opérant depuis la Suisse peut gérer des transactions entre une entreprise européenne et une société écran établie à Hong-Kong, sans prendre de risque juridique[97]. Toutefois, cette mobilité géographique reste en grande partie théorique. En effet, pour pouvoir fonctionner, les courtiers s'appuient sur des entreprises établies dans un pays donné avec lesquelles ils ont des contacts particuliers[98]. Les intermédiaires eux-mêmes sont sans doute extrêmement flexibles, mais l'environnement de travail dont ils dépendent ne l'est pas.

En matière financière, les organisations d'acquisition utilisent un réseau de sociétés qui leur permet de dissimuler l'origine des fonds employés et par là même la finalité des opérations. Une partie de ces institutions se trouvent plus ou moins directement sous leur contrôle. Outre l'utilisation de paiements en numéraire, permettant d'échapper à la vigilance des services de surveillance financière, le recours aux virements de préférence

[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] Quelques employés et parfois uniquement une adresse postale. Il n'est pas rare que les courtiers créent des sociétés champignons pour mener quelques opérations spécifiques.

[97] http://www.nisat.org/publications/armsfixers/Chapter1.html

[98] C'est le cas notamment pour le transport des biens ou encore les opérations financières.

aux lettres de crédit semble également être devenu plus fréquent[99]. En effet, l'ouverture d'une lettre de crédit nécessite le dépôt de documents, en particulier le contrat entre le vendeur et l'acheteur dont la complétion permet le paiement au vendeur. La lettre de crédit laisse donc une trace qui peut être détectée par les services de surveillance financiers et permet de déterminer les biens ou services échangés. Un virement bancaire, en revanche, n'est pas lié au moindre élément documentaire et s'avère en conséquence difficile à exploiter même s'il est détecté. Cette méthode permet probablement de financer les opérations à la fois au sein du réseau (activités des sociétés écrans par exemple) mais également avec les intervenants extérieurs.

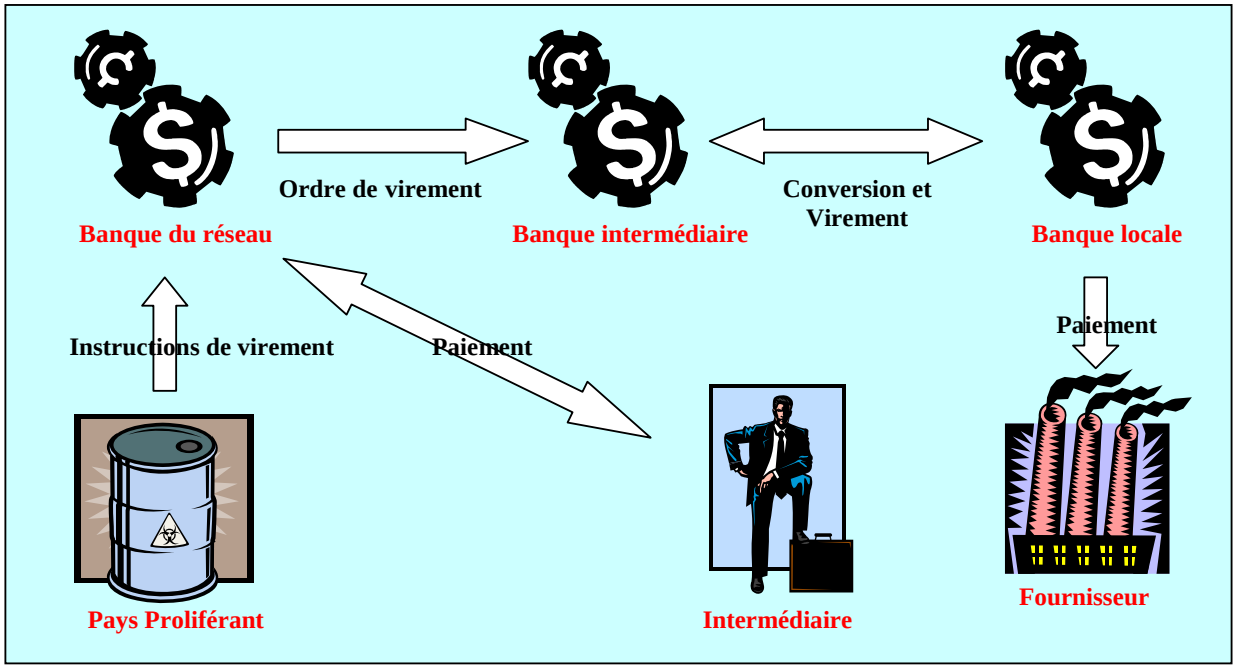



**Figure 6 : Schéma de fonctionnement d'une transaction bancaire associée à l'acquisition d'un bien proliférant**

Malgré la diversification des intermédiaires financiers, les réseaux de prolifération semblent continuer à s'appuyer uniquement sur une poignée de banques, véritables centres névralgiques de leurs activités confidentielles. La banque centrale syrienne fût par exemple l'un des points de passage obligés à la fois pour le financement du réseau d'acquisition irakien mais également pour les bénéfices obtenus au travers de la vente illicite de produits pétroliers dans le cadre du contournement du système « pétrole contre nourriture »[100]. De même, la *Banco Delta Asia* servait probablement à la fois de réserve financière à Kim Jong Il[101] – alimentée à la fois par les divers trafics et par de généreux donateurs – mais également à entretenir le réseau d'acquisition de Pyongyang. En provoquant le gel des avoirs nord-coréens gérés par cette banque, le département du Trésor américain a obtenu une véritable réaction en chaîne sur les établissements

[99] Entretiens de l'auteur, juin 2006.

[100] Rapport de l'Iraq Survey Group (ISG).

[101] « U.S. now Believes Macau Bank Account was Kim Jong Il's « personal » slush fund », *East-Asia Intel*, July 26, 2006.

financiers situés en aval[102]. Toutefois, tout porte à croire que les réseaux possèdent la capacité de réorganiser leur structure financière en cas de neutralisation de l'un de leurs centres, en s'appuyant sur des établissements de confiance. Ainsi, il semblerait que Pyongyang ait déjà engagé une telle démarche afin de remplacer la *Banco Delta Asia* par une entité singapourienne[103]. Le régime nord-coréen chercherait également à ouvrir des comptes dans des banques russes ou vietnamiennes sous des noms d'individus plutôt que de sociétés[104].

### ➡ Vulnérabilités d'un réseau de fournisseur

En établissant les critères de vulnérabilité des réseaux de fournisseurs, nous avons défini une série de paramètres qui paraissent aussi bien applicables aux organisations d'acquisition.

La particularité de ces derniers toutefois est que, vu leur caractère institutionnel[105], donc leur taille et leur déconcentration fonctionnelle, ils présentent une vulnérabilité plus importante au niveau technique qu'en termes structurels. La capacité des États concernés à définir précisément leur besoin, à trouver les fournisseurs capables d'y répondre de façon satisfaisante et à organiser efficacement l'interface entre la branche d'acquisition et l'utilisateur final représente la principale difficulté. Le niveau d'avancement du programme d'armes concerné joue donc un rôle essentiel pour déterminer l'efficacité du réseau.

Ainsi, un acteur n'ayant aucune expérience technique ou technologique qui devrait acquérir des capacités sur étagère ou souhaiterait établir une compétence propre, devra s'appuyer sur des réseaux de fournisseurs capables de proposer une offre complète. Par exemple, dans le domaine des missiles, un tel État pourrait se tourner vers la Corée du Nord, la Chine ou la Russie. Dans ce cas de figure, le système d'acquisition peut être relativement simplifié par rapport au modèle décrit précédemment, la majeure partie des opérations étant prises en compte par le fournisseur. Sa vulnérabilité tient donc davantage à la capacité nationale d'assimiler les technologies fournies – y compris la maintenance des systèmes ou encore leur emploi opérationnel dans le cas de missiles – qu'à son organisation. En termes financiers, le réseau peut se limiter au paiement direct du fournisseur sous la forme la plus discrète (en liquide ou par virement bancaire) voire même recourir à l'ouverture de lettres de crédits en privilégiant les contacts entre ses propres établissements bancaires et ceux du réseau de fournisseur. De même, s'il peut faire appel à des courtiers ou à des intermédiaires, le contact direct avec ceux-ci lui permet de réduire considérablement sa visibilité vis-à-vis de l'extérieur et les risques de neutralisation temporaire de son activité. Parmi les réseaux d'acquisition connus, c'est celui de la Libye qui semble le plus correspondre à ce modèle : par exemple, pour l'acquisition d'une capacité d'enrichissement, les services libyens ont engagé des

[102] Ainsi la Banque Centrale Chinoise aurait également procédé au gel des avoirs nord-coréens tout comme plusieurs banques européennes. Ibid.

[103] « North Korean counterfeiters back in business, via Singapore bank », *East-Asia Intel*, August 9, 2006.

[104] « North Korean opens bank accounts in Russia to avoid scrutiny of leadership cash flow », *East-Asia Intel*, September 6, 2006.

[105] Nous laissons de côté les organisations privées d'acquisition, comme les sectes ou les mouvements terroristes, pour lesquels tant l'échelle des moyens consacrés que le caractère totalement illégal de leur activité sortent du cadre de cette étude.

contacts directs avec A. Q. Khan, le paiement s'effectuant, du moins en partie, en liquide.

Pour les États possédant des programmes nationaux, l'acquisition de certains composants clefs nécessite de pouvoir faire appel à des États fournisseurs qui ne sont pas proliférants[106]. Dans ce cadre, l'établissement d'un maillage international de sociétés et de personnes agissant au profit de l'activité d'acquisition, conformément au modèle développé, est essentiel. Du reste, cette partie du réseau constitue une cible possible pour les organisations – nationales ou internationales – chargées de lutter contre la prolifération. Pour autant, c'est bien le niveau de compétence technique du pays proliférant qui va être déterminant pour l'efficacité de la fonction d'acquisition. On peut ainsi établir une distinction entre les États ayant une simple capacité systémique (la possibilité de produire un système à partir de ces principaux composants) et ceux capables de fabriquer les composants clefs du système[107] :

- Les États ayant uniquement une capacité systémique doivent acquérir certains composants complets spécifiques, dont les tentatives d'acquisition s'avèrent plus facilement détectables. S'ils peuvent se tourner vers des réseaux de fournisseurs pour y accéder – ces derniers apportant leur propre capacité technique – ils sont parfois obligés de faire appel à des fournisseurs extérieurs. Cette situation crée une double vulnérabilité pour le système d'acquisition :
  - La coordination entre la branche technique et le service d'achat devient essentielle. Une défaillance dans ce domaine peut entraîner par exemple l'acquisition d'un produit trop éloigné des spécifications de l'utilisateur pour être utile[108].
  - Une dépendance envers un nombre restreint de fournisseurs : dans les domaines considérés (nucléaire ou missiles) les sociétés possédant le savoir-faire nécessaire pour produire des sous-systèmes complets sont peu nombreuses[109]. De plus, les biens considérés sont relativement contrôlés par les autorités nationales s'agissant de technologies relevant, le plus souvent, du domaine militaire.
- Les États capables de produire les composants clefs du système peuvent s'appuyer sur l'acquisition de biens élémentaires de nature duale, dont l'achat est moins visible pour les services de contrôle. Ce degré de maîtrise technique permet de réduire considérablement le risque de détection des activités du réseau.

A la lumière de ces éléments, il apparaît que l'interaction entre les réseaux de fournisseur et les réseaux d'acquisition joue un rôle particulier en matière de prolifération. Comme nous l'avons d'ailleurs vu dans les cas d'espèce étudiés précédemment, plusieurs relations se sont tissées entre réseaux depuis le milieu des années 1990 qui semblent indiquer l'apparition d'une forme de mondialisation des échanges proliférants.

[106] Que l'on qualifie d'États sources dans la suite de l'étude.

[107] Une telle distinction élémentaire est détaillée pour le domaine nucléaire dans un article de William C. Potter, « The diffusion of Nuclear Weapons », in « The Diffusion of Military Technology and Ideas », Standford University Press, 2003, pp. 169-170.

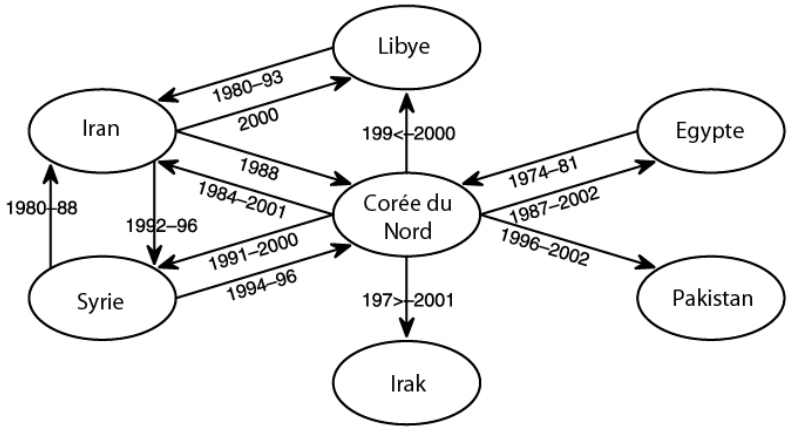
[108] Rappelons l'exemple de l'acquisition en 1995 par les services secrets irakiens de centrales inertielles pour missiles lancés de sous-marins, lesquelles s'étaient avérées inutilisables par les centres techniques travaillant sur le programme de missile.

[109] Par exemple, pour ce qui concerne les systèmes de navigation (complets et utilisables pour des missiles balistiques), il n'existe en Europe que deux sociétés : Thales et SAGEM.

### *1.2.3 – Interactions entre réseaux : vers une mondialisation de la prolifération*

Dans les exemples que nous avons étudiés précédemment, les organisations impliquées ont mené deux types d'opération, soit avec des entreprises implantées dans des États non proliférants, soit avec d'autres réseaux de prolifération.

**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.

Dans ce dernier cas, le mouvement d'une partie des flux matériels, immatériels et financiers peut s'avérer insaisissable dans la mesure où ils n'impliquent pas le recours à des sociétés établies légalement. Toutefois, la nature même des réseaux de prolifération fait que leurs échanges ne peuvent être réalisés sans le recours à des sociétés extérieures. Ceci vient, en particulier, du fait que les fournisseurs connus ne sont pas en mesure de proposer un produit qui soit totalement indigène. Par exemple, après que le réseau Khan se soit détaché de l'organisation d'acquisition du programme nucléaire pakistanais, il a dû se tourner vers des fournisseurs étrangers pour certains composants. A la différence des modèles théoriques décrits ici, les réseaux de prolifération ne peuvent donc pas fonctionner sans interaction avec des entités qui ne sont pas proliférantes dans la mesure où ils poursuivent à la fois des activités d'acquisition et de vente.

L'établissement de réseaux tissant des liens entre les organisations proliférantes constitue toutefois une évolution inquiétante dans la mesure où elle tend à renforcer la résistance de chacune des organisations à des perturbations extérieures. Il est particulièrement frappant, dans le domaine des missiles balistiques, de constater que les coopérations qui se sont tissées entre les réseaux dans les années 1980-1990 tendent à donner une place de moins en moins centrale à la Corée du Nord au profit de coopérations croisées entre ses anciens clients. D'une structure en étoile, centrée autour du réseau nord-coréen, on aboutit aujourd'hui à une structure décentralisée plus dynamique, mais également plus difficile à neutraliser[110]. D'autres entités se rattachent également à ce réseau de réseaux de façon plus périphérique, comme par exemple la Chine ou la Russie.

Pour ce qui concerne la prolifération nucléaire, force est de constater que la structure des relations entre réseaux reste centralisée avec au cœur le réseau pakistanais.

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

Toutefois, le développement des capacités nucléaires de l'Iran et de la Corée du Nord pourrait à terme conduire à une décentralisation sur le modèle du cas balistique. L'une des particularités du réseau nucléaire tient au fait que l'organisation centrale détient et propose les connaissances et le savoir-faire nécessaire aux autres. En définitive, la structuration des réseaux d'organisation correspond en grande partie au niveau de diffusion du savoir – technologies, connaissances, expérience[111] – entre les diverses entités impliquées. Il faut craindre à terme que le réseau global nucléaire finisse par se décentraliser du fait de l'émergence de nouveaux acteurs capables de diffuser ou d'échanger entre eux, sans passer par le centre, leurs connaissance et savoir-faire.

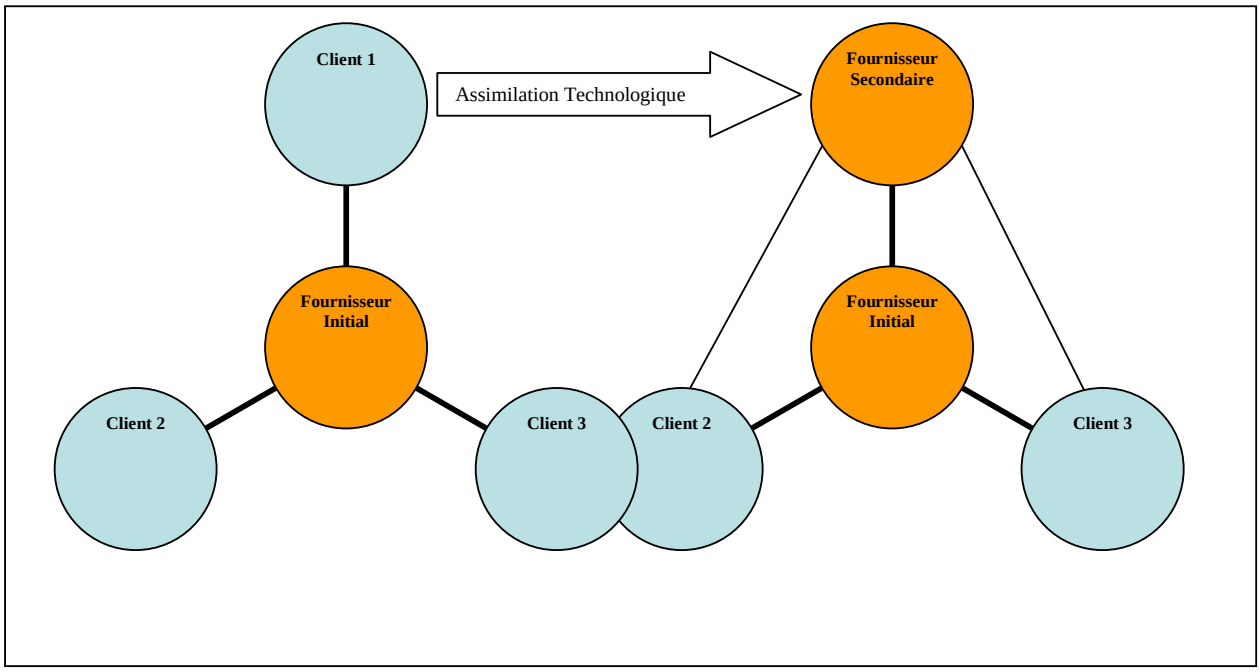



**Figure 7 : Évolution d'un Réseau sous l'Influence de l'Assimilation de Technologies**

Outre l'interaction technique entre les réseaux, il convient de souligner que d'autres liens ont également tendance à se développer au sein du petit monde de la prolifération. Tout d'abord, ils concernent les agents des réseaux au sein des États sources[112], c'est-à-dire les intermédiaires, courtiers et autres hommes de paille qu'emploient les réseaux pour mener une partie de leurs opérations. Même si la plupart des réseaux font appel à leurs propres agents pour mener des opérations à l'étranger, il n'est pas rare qu'ils fassent appel aux mêmes intermédiaires. Ainsi, il semble que le réseau d'acquisition nucléaire indien se soit appuyé sur des entités sud-africaines qui ont également travaillé

[111] L'expérience constitue ce qui ne peut s'apprendre que par les essais, échecs et tâtonnements d'un programme particulier. Comme le montre William Potter – dans une moindre mesure Alexander Montgomery – c'est que la diffusion des technologies entre pays n'est pas uniquement assurée par la transmission de données, de composants mais nécessite également que les receveurs les assimilent. Or, nous sommes là face à un phénomène sur lequel influent des facteurs politiques, historiques, techniques et économiques qui dépendent des pays concernés. W. Potter, « The diffusion of Nuclear Weapons », op. cit.

[112] On désigne ainsi les États dans lesquels sont implantées des sociétés dont les réseaux de prolifération tentent d'acquérir les biens ou technologies. Par extension, on y ajoute les paradis fiscaux, les États de pavillon de complaisance et les pays servant de plaque tournante aux trafics.

au profit du réseau Khan[113]. Les réseaux peuvent également être amenés à fédérer leurs efforts d'acquisition dans les États sources dans le cadre d'un programme commun. Pour le développement du missile argentino–égypto–irakien Condor-2 dans les années 1980, la gestion du programme était assurée par une société transnationale, le groupe CONSEN, chargé aussi bien des aspects financiers ou de la supervision technique du programme, que des activités d'acquisition à l'étranger. Cette société avait fait appel à des intermédiaires, dont notamment Abdel Kader Helmy dont le rôle consistait à acheter aux États-Unis certains composants nécessaires au programme[114]. La mise en place de la *joint venture* russo-irakienne ARMOS dans le cadre des efforts d'acquisition du réseau irakien s'inscrit dans une logique similaire[115].

Au vu de l'accroissement des coopérations croisées entre pays proliférants, la mise en commun d'une partie des opérations d'acquisition semble être incontournable. Elle pourrait prendre la forme d'une mutualisation ponctuelle des moyens logistiques et financiers permettant d'améliorer l'efficacité de la gestion des flux matériels et immatériels entre les réseaux concernés. L'utilisation des moyens de transport d'un réseau au profit d'une opération menée par un autre ne peut pas être exclue[116], tout comme l'utilisation d'établissements bancaires opérant pour un réseau au profit d'un autre[117]. Mais si ces rapprochements opérationnels peuvent s'accroître, ils seront en tout état de cause limités du fait des vulnérabilités qu'ils induisent sur les filières nationales. Il s'agit en effet pour les divers acteurs du marché d'éviter que la neutralisation complète ou partielle d'un réseau ami ne conduise à celle de sa propre organisation. Par ailleurs, comme le souligne Alexander Montgomery, même si les réseaux ont tendance à se rapprocher du fait de la similarité de leur structure et des contacts qu'ils peuvent entretenir avec un fournisseur commun, l'existence de compétition entre eux voire de mauvaises relations politiques diminue le risque de les voir coopérer directement[118].

Dès lors, les relations que peuvent entretenir les réseaux avec le monde extérieur devraient continuer à être un élément déterminant de leur existence et de leur fonctionnement.

[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] Son arrestation, en 1988, a largement influencé l'abandon du programme par l'Égypte. http://nti.org/e_research/profiles/Egypt/Missile/index.html

[115] Voir § 1.1.2.1.

[116] Certains réseaux bénéficient par exemple d'une flotte de commerce importante qu'ils pourraient mettre à disposition de leurs clients ou fournisseurs pour échapper aux interceptions menées dans le cadre de la PSI. Voir B. Gruselle, « Missiles de croisière et stratégies d'anti-accès », rapport d'étude FRS, décembre 2005, p. 48.

[117] Ainsi, une compagnie aérienne chinoise Great Wall Airlines, liée à la société chinoise Great Wall Industries, a été sanctionnée par le département du Trésor américain pour avoir servi à transporter des composants vers l'Iran et la Corée du Nord. « U.S. sanctions Chinese airliner for freighting WMD to Iran, N. Korea », *East-Asia Intel*, 6 septembre 2006.

[118] Alexander H. Montgomery, « Ringing in Proliferation », op. cit., p. 177.

### *1.2.4 – Interactions avec le monde extérieur et capacité d'adaptation des réseaux*

Outre les interactions qu'ils développent entre eux, les réseaux de prolifération entretiennent des rapports étroits avec d'autres acteurs. Il peut s'agir de liens commerciaux, fonctionnels (par exemple logistiques) ou encore politiques. En effet, comme nous l'avons vu, les réseaux de prolifération ne fonctionnent pas en boucle fermée : leur dépendance technique vis-à-vis des États sources, la nécessité de mouvoir leur capitaux pour réaliser leurs opérations, la gestion des flux matériels ou encore les tentatives de neutralisation influent directement sur leurs opérations.

Les intervenants extérieurs dans les activités d'un réseau sont de deux principaux types :

- Intervenants amicaux : outre les clients, certains pays, institutions, acteurs, agissent au profit des réseaux pour des motifs politiques ou économiques. A titre d'exemple, le réseau irakien a pu profité d'un soutien de la part de pays voisins pour l'établissement de comptes bancaires destinés à gérer ses transactions bancaires. Les intermédiaires n'agissant pas sous le contrôle direct et exclusif du réseau font également partie de cette catégorie.
- Les acteurs hostiles : qu'il s'agisse des groupes de fournisseurs ou encore des États cherchant à les neutraliser, les réseaux se trouvent confronter à des actions susceptibles de diminuer leur efficacité ou de miner leurs opérations. Les États-Unis jouent par exemple un rôle clef en matière de lutte contre les réseaux, notamment par le lancement de la *Proliferation Security Initiative* ou encore dans le cadre de leurs efforts de démantèlement des opérations financières. De même, les efforts des services de renseignement des pays occidentaux pour démanteler les organisations effectuant des trafics font peser un risque sur l'existence des réseaux de prolifération. La possibilité de voir leurs opérations mises à jour par des actions de renseignement – y compris éventuellement par l'infiltration – n'est pas inexistante. Ainsi, Urs Tinner, qui avait conduit les travaux en Malaisie au profit d' A. Q. Khan dans le cadre du contrat libyen, pourrait avoir agit au profit de la CIA[119] et avoir fourni à l'agence américaine des informations concernant les activités du réseau. En tout état de cause, cette situation oblige en théorie les organisations proliférantes à être réactives et dynamiques, c'est-à-dire capables d'une part de protéger leurs opérations pour éviter qu'elles soient découvertes et d'autre part d'être en mesure de les réorganiser de façon à permettre leur continuité en cas de perturbation de l'environnement. Or, force est de constater que face à diverses difficultés, les réseaux connus n'ont pas toujours la capacité de s'adapter. Plus précisément, il semble judicieux pour l'analyser de séparer les difficultés en trois domaines :
  - Les difficultés d'ordre technique : l'évolution des systèmes de contrôle des exportations tend à élargir le domaine des composants et technologies contrôlés (même si tous les pays n'ont pas des normes identiques). De fait, elle a déjà conduit les réseaux à concentrer leurs acquisitions sur des composants de plus en plus élémentaires pour échapper à la vigilance des organisations chargées du contrôle. Mais leur compétence technique limite effectivement leur capacité à s'adapter à l'élargissement du spectre des composants contrôlés. Ainsi, si cette tendance se poursuit, ils seront amenés à conduire certaines de leurs acquisitions

[119] « The Double Game in the Nuclear Poker », *Focus*, March 15, 2005.

de façon de plus en plus illégale, multipliant les risques pour leurs agents et intermédiaires[120].

⇨ Les problèmes d'ordre logistique : la mise en place des filières destinées à transporter les biens acquis à l'étranger repose le plus souvent sur le recours à des sociétés de transport ou d'affrètement n'appartenant pas au réseau[121]. Dans le cas où l'État source appartient à un réseau de prolifération et que les moyens employés lui appartiennent, le risque de perturbation est faible[122]. En revanche, dans le cas où les biens sont transportés par une société privée sur un navire ou un avion-cargo commercial n'appartenant pas à un État proliférant, plusieurs événements – par exemple interception de la cargaison, en haute mer ou au-dessus de l'espace aérien national d'un acteur hostile – peuvent exposer l'opération et le fonctionnement du réseau acheteur. Pour autant, ce type de perturbation ne paraît pas durable dans la mesure où elle n'expose *a priori* que la société écran à laquelle les biens sont destinés. Le réseau concerné peut donc réagir rapidement en utilisant d'autres sociétés écrans sous sa coupe (ou éventuellement en en créant de nouvelles). Qui plus est, l'absence de contrôle externes ou de code de bonne conduite pour les professions logistiques – transport et affrètement – autant que le caractère économiquement profitable de cette activité économique rend les entreprises concernées assez peu regardantes sur l'identité ou la nature de leur client[123]. La mise en cause ou la neutralisation durable d'intermédiaires implantés à l'étranger paraît plus gênante pour un réseau (ou un réseau de réseaux). En effet, même s'ils sont remplaçables, les courtiers jouent comme nous l'avons vu un rôle central dans le fonctionnement des réseaux et leur neutralisation peut nuire durablement à leurs fonctionnements. Toutefois, pour obtenir cet effet, encore faut-il que les États soient en mesure de poursuivre et d'arrêter les intermédiaires mis en cause.

⇨ Les difficultés de nature bancaire : le fonctionnement des réseaux de prolifération repose sur la possibilité pour ces derniers de mouvoir des fonds entre eux-mêmes, leurs agents et leurs clients et fournisseurs. Une partie de ces transactions s'opèrent au sein du système bancaire international et, comme nous l'avons vu, les organisations proliférantes font appel à des établissements bancaires privés ou publics pour réaliser ces opérations. Ainsi, une partie des fonds irakiens destinés à alimenter le réseau d'acquisition transitait sur des comptes individuels ouverts dans des banques syriennes, libanaises ou européennes. Le gel des avoirs déposés dans ces banques « de confiance » est de nature à perturber profondément le fonctionnement des réseaux dans la mesure où, outre les pertes financières associées[124], il interdit pratiquement la rémunération des intermédiaires et fournisseurs, dont la participation reste essentiellement motivée par des questions

[120] Toutefois, pour parvenir à cette situation, il est nécessaire que les organisations chargées du contrôle soient capables de suivre efficacement des biens et technologies de plus en plus nombreux et variés. Elle nécessite également une harmonisation internationale des critères et de l'efficacité des systèmes de contrôle (cf. infra et chapitre 2).

[121] Entretiens de l'auteur, novembre 2006.

[122] Par exemple, c'est le cas nord-coréen. L'emploi de voies de communication diplomatiques entre également dans ce cas de figure.

[123] Entretiens de l'auteur, novembre 2006.

[124] Qui peuvent être très importantes si ce gel touche les banques se trouvant au cœur des activités financières. Cf. supra.

économiques. De plus, il peut créer des effets de cascade sur les États dans lesquels sont implantés des établissements financiers se trouvant en aval et qui, pour éviter d'être sanctionnés, procèdent également à des actions similaires[125]. Selon le niveau auquel se trouve l'établissement financier concerné (cf. figure 8), la difficulté de récupération pour le réseau est plus ou moins importante. Ainsi, la neutralisation des banques locales qui ne gèrent qu'une infime partie des ressources du réseau ne pose pas de problèmes insurmontables dans la mesure où l'on peut supposer que les flux financiers peuvent transiter par d'autres établissements du même niveau. En revanche, la neutralisation de banques intermédiaires est plus fâcheuse puisqu'elles gèrent à la fois des sommes plus importantes mais également parce qu'elles contrôlent les flux vers une série d'autres acteurs locaux. Qui plus est, à la différence des établissements se trouvant sous le contrôle plus ou moins direct du réseau, leur neutralisation paraît possible, s'agissant généralement de sociétés commerciales sensibles à la menace d'éventuelles sanctions commerciales, ou se trouvant sous la juridiction de gouvernements sur lesquels des pressions politiques peuvent être exercées[126]. Pour les réseaux de prolifération, remplacer les établissements intermédiaires compromis peut poser d'importantes difficultés : cela nécessite de reconstruire en grande partie le réseau mais également de trouver une banque de confiance susceptible de gérer les transactions avec les banques locales. On perçoit bien par exemple ces difficultés dans le cas de la gestion des avoirs nord-coréens placés à la *Banco Delta Asia*. Pyongyang semble avoir le plus grand mal à trouver une société qui prendrait le risque de reprendre ce type d'activité à son profit.

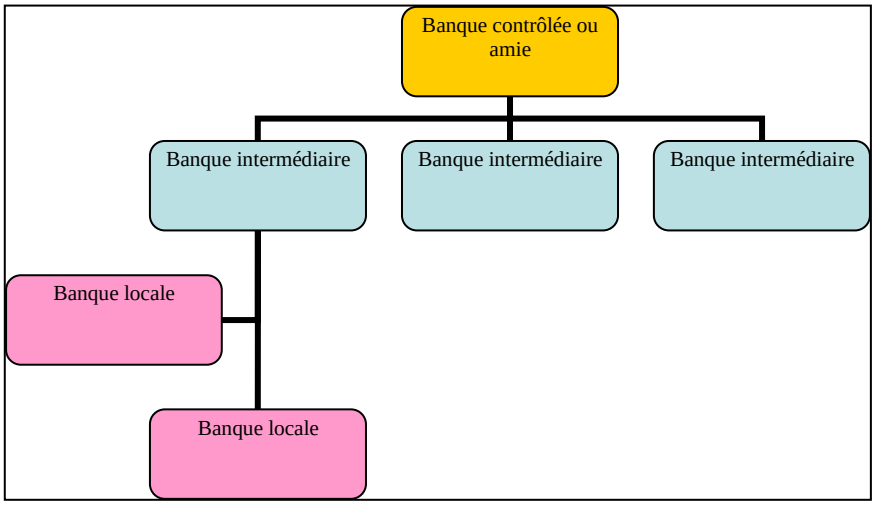



**Figure 8 : Niveau de sensibilité des établissements financiers opérant au profit d'un réseau**

[125] Entretiens de l'auteur, décembre 2006.

[126] Ainsi, le fait que la banque centrale chinoise décide d'enquêter sur les avoirs nord-coréens déposés en Chine montre la sensibilité de ces établissements relais à des pressions économiques.

L'influence du développement du commerce mondial sur les réseaux de prolifération fait également partie des questions qui se posent concernant l'évolution de ce phénomène et son interaction avec les acteurs extérieurs. Si la mondialisation et la dématérialisation des échanges ne sont pas les causes de l'apparition des réseaux, elles ont contribué à l'évolution de leur fonctionnement[127].

D'abord parce que les technologies sont devenues plus accessibles du fait de l'essor des technologies de l'information. Ainsi, il est possible pour une organisation de fournisseur de transférer des informations à son client rapidement et de façon confidentielle et de même à un réseau d'acquisition d'obtenir un soutien technique de façon discrète. Les bénéfices acquis par les réseaux du fait de la dématérialisation des échanges financiers sont plus relatifs. D'un côté, elle permet de mouvoir rapidement et efficacement des sommes d'argent entre les établissements financiers, les agents et les fournisseurs ou clients. La discrétion de ces échanges reste toutefois sujette à interrogation dans la mesure où les échanges informatiques peuvent être plus facilement suivis et plus efficacement traités par les services de renseignement que les échanges papiers. Toutefois, les trafics sont plus difficiles à détecter par ce biais en l'absence de socle documentaire associé à une transaction[128].

Ensuite, parce que l'accroissement des échanges permet de dissimuler plus facilement les trafics au cœur de transactions légitimes[129]. Rien que pour le commerce maritime, la quantité de biens transportée par mer a crû, entre 1970 et 2005, de 2 500 à 5 800 millions de tonnes[130], cette croissance se concentrant en particulier dans la zone Asie–Pacifique. En particulier, le transport par navires porte-conteneurs a connu une forte croissance permise à la fois par l'augmentation de la capacité d'emport des bateaux mais également par la modularité de ce type de transport[131]. Pour les réseaux de prolifération, le développement de ce mode de transport présente plusieurs intérêts :

- Les principaux opérateurs du secteur (affréteurs, transporteurs, manutentionnaires) sont plus nombreux et ne possèdent pas aujourd'hui les moyens matériels permettant de garantir la traçabilité des chargements. Il est donc possible pour un prolifèrant de dissimuler un composant sensible dans un conteneur et de limiter ainsi sa possibilité de détection.
- Le transbordement permet de jouer sur la nature plus ou moins laxiste du contrôle des marchandises en transit dans les grands « *hubs* » commerciaux. Par exemple, il pourra être avantageux de choisir de prendre livraison de sa marchandise à Dubaï ou Taiwan plutôt qu'à Marseille ou Singapour, où les contrôles sont plus stricts.

L'essor des échanges mondiaux a enfin largement contribué à la diffusion des technologies à un plus grand nombre d'acteurs industriels. Il est donc devenu possible pour les réseaux de prolifération de faire appel à des entreprises disposant des savoir-faire ou des

[127] J. Caves, « Globalization and WMD Proliferation Networks : The Policy Landscapes », *Strategic Insights*, Vol. V, Issue 6, July 2006.

[128] Cf. § 1.2.2 du présent document.

[129] Selon la banque mondiale, la croissance du commerce de marchandise s'établit à 8,9 % en 2005, elle était de 11,8 % en 2004.

[130] http://www.ac-rennes.fr/pedagogie/hist_geo/ResPeda/mondialisation/commerce/cemaritimegraphes.htm

[131] A. Frémont, « Les réseaux maritimes conteneurisés : épine dorsale de la mondialisation », *INRETS*, octobre 2005, p. 4.

produits recherchés et qui sont implantées dans des États dont les dispositifs de contrôle sont moins efficaces qu'ailleurs. L'utilisation de la société malaisienne SCOMI par le réseau Khan repose, par exemple, sur cette logique. De fait, la diffusion internationale des technologies contribue à limiter l'impact sur les réseaux de prolifération de l'élargissement par certains États des listes de biens contrôlés à l'exportation.

En définitive, la mondialisation représente, pour les réseaux de prolifération existants, une opportunité à la fois de perfectionner leur fonctionnement mais également des outils pour se protéger des tentatives des États pour les neutraliser. Toutefois, pour exploiter ces outils, les filières doivent jouir de capacités techniques et d'une organisation fonctionnelle adaptée. Par exemple, un nouvel acteur proliférant, ne disposant pas de connaissances suffisantes, ne pourra pas mettre à profit la diffusion des technologies, n'étant pas à même, à partir de composants élémentaires, de développer et de produire un système complet. Pour y parvenir, il devra faire appel à un fournisseur capable de le faire – tout comme la Libye avait fait appel au réseau Khan pour acquérir sur étagère une capacité d'enrichissement.

### *1.3 – Perspectives de développement des réseaux d'acquisition illégaux*

Tout porte à croire que la prolifération des technologies, biens et savoir-faire liés aux armes de destruction massive et à leur vecteurs fonctionne peu ou prou comme un marché. L'existence d'une demande appelle la création d'une offre, cette dernière étant plus ou moins complète en termes techniques et logistiques.

Mais l'adéquation entre les besoins des acheteurs et les capacités du marché à y répondre est encore loin d'être assurée. Malgré l'efficacité de son organisation et ses efforts incessants, le réseau d'acquisition irakien n'a pas été capable de répondre complètement aux besoins exprimés par le régime. La pression créée par le régime d'inspection et de contrôle des Nations Unies n'est bien sûr pas étrangère à cette faillite. En obligeant le système d'acquisition irakien à opérer selon des modes totalement illégaux et les plus discrets possibles, elle l'a probablement empêché de se rapprocher de fournisseurs capables de répondre efficacement au besoin. Ainsi, il est vraisemblable que la rupture des négociations entre Bagdad et le réseau Khan ait été entraînée par les craintes des services secrets irakiens d'une découverte de l'affaire.

Toutefois, l'apparition de réseaux de fournisseurs capables d'offrir un produit complet et techniquement crédible est de nature à rendre le marché plus efficace et en conséquence à accroître les risques de prolifération. Le cas de la privatisation du réseau A. Q. Khan apparaît particulièrement inquiétant, dans la mesure où pour la première fois – dans le domaine nucléaire – une organisation fonctionnant sur une base essentiellement commerciale est en mesure de proposer une capacité complète hors du contrôle des autorités nationales. Il est à craindre que d'autres organisations de ce type existent ou apparaissent. C'est déjà d'ailleurs le cas dans le domaine des missiles avec le réseau nord-coréen, qui pourrait étendre ses activités à la fourniture de capacités nucléaires. Mais le caractère étatique de ce réseau en limite toutefois en partie la nuisance.

En effet, une autre tendance inquiétante se dessine avec une entrée possible sur le marché d'acheteurs non étatiques, par exemple des groupes terroristes. Les efforts de la secte Aum Shirnikyo pour acquérir plusieurs tonnes de précurseurs chimiques afin de

fabriquer des armes préfigurent une telle évolution[132]. Au vu de la nature de l'activité terroriste du début du XXI^e siècle, l'émergence d'une micro-prolifération des armes de destruction massive est à craindre, qui serait alimentée par des fournisseurs–systémiers[133] eux aussi non étatiques ou plutôt détachés des États, sur le modèle Khan.

En définitive, même s'il reste important de faire pression sur la demande – en particulier par le biais des actions de non-prolifération – il convient aujourd'hui d'accélérer le développement d'une réponse efficace visant l'évolution de l'offre. Il ne s'agit pas là de chercher à neutraliser systématiquement les fournisseurs proposant des composants élémentaires, même si cela est souhaitable, mais bien d'empêcher l'apparition et le développement de réseaux privés capables et disposés à livrer un système complet à n'importe quel client. Ce sont effectivement ces organisations qui présentent la plus grande menace en termes de non-prolifération.

[132] Scott Jones, « Black Market, Loopholes and Trade Controls: The Mechanics of Proliferation », 2005 Carnegie International Non-Proliferation Conference, November 8, 2005.

[133] C'est-à-dire capable de proposer une offre système, complète.

## 2 – Quels moyens et quelles politiques pour neutraliser les réseaux de prolifération ?

Pour répondre aux développements des activités des réseaux de prolifération, le seul renforcement des outils de non-prolifération actuellement disponibles apparaît comme insuffisant. En effet, il s'agit dans ce cadre à la fois de réduire la demande mais également de neutraliser les pourvoyeurs de biens et de technologies qui l'alimentent. En outre, demande comme offre risquent de se complexifier en s'étendant à des acteurs privés sur lesquels la politique de non-prolifération n'a que peu de prise.

De façon générale, l'efficacité de la lutte contre les réseaux de prolifération devrait reposer sur trois piliers :

- **La cartographie des activités des réseaux**. Caractériser la structure d'un réseau donné permet de déterminer quels sont les acteurs essentiels, leurs rôles au sein de l'organisation et ainsi de choisir les meilleurs cibles pour les actions visant à le neutraliser durablement.
- **La neutralisation pérenne** des fonctions clefs des réseaux : en mettant un terme à certaines activités logistiques, financières ou techniques d'un réseau ou en neutralisant des acteurs clef de son fonctionnement (sociétés ou banques intermédiaires, coordonnateur..).
- **L'interruption des flux essentiels** qu'il s'agisse des transferts matériels, immatériels ou financiers, peut dégrader durablement le fonctionnement des réseaux.

La mise en place d'une politique de neutralisation des réseaux de prolifération doit donc s'appuyer sur le renforcement d'une série d'outils dont le fonctionnement est complémentaire. Tout d'abord, elle doit faire appel à l'existence d'une fonction de détection dont le rôle est non seulement d'identifier des flux suspects mais également de mettre à jour l'organisation du réseau ainsi que ces acteurs clefs. S'appuyant sur cette capacité, deux types de mesures sont susceptibles d'être mises en œuvre :

- **La répression** vise à neutraliser l'activité des agents du réseau ou à empêcher la conclusion des opérations entreprises par ceux-ci. Il peut s'agir par exemple d'interdire l'accès du réseau à des banques intermédiaires ou relais, ou encore d'empêcher *a priori* l'exportation de biens ou le transfert de technologies organisés au profit du réseau ou d'un de ses clients.
- **L'interdiction** consiste à bloquer des transferts ou opérations en cours. Elle peut être effectuée dans un cadre juridique (saisie en douanes, gel de compte, sanctions) ou militaire (interception de cargaison en mer).

Dans cette partie, il s'agit de déterminer comment peuvent fonctionner ces outils face aux modèles de réseaux étudiés précédemment. En particulier, l'adaptation des moyens de détection, de répression et d'interdiction à l'évolution des trafics proliférants doit être évaluée afin de proposer des options possibles pour en améliorer l'efficacité.

La coordination des approches nationales et internationales en matière de lutte contre les réseaux constitue également un enjeu de taille. En effet, l'exploitation des mécanismes du commerce international permet aux réseaux d'échapper en partie à d'éventuels

renforcements des moyens des États. C'est pourquoi, le développement d'outils internationaux de lutte contre les réseaux de prolifération s'impose, qui pourrait s'appuyer sur des moyens existants. Mais il s'agit également de s'interroger sur les démarches qui doivent être entreprises pour amener les divers acteurs économiques à prendre mieux en compte cette question dans leur gestion quotidienne. Ce d'autant que le phénomène de privatisation des activités de prolifération devrait les conduire à jouer un rôle grandissant dans le fonctionnement des réseaux.

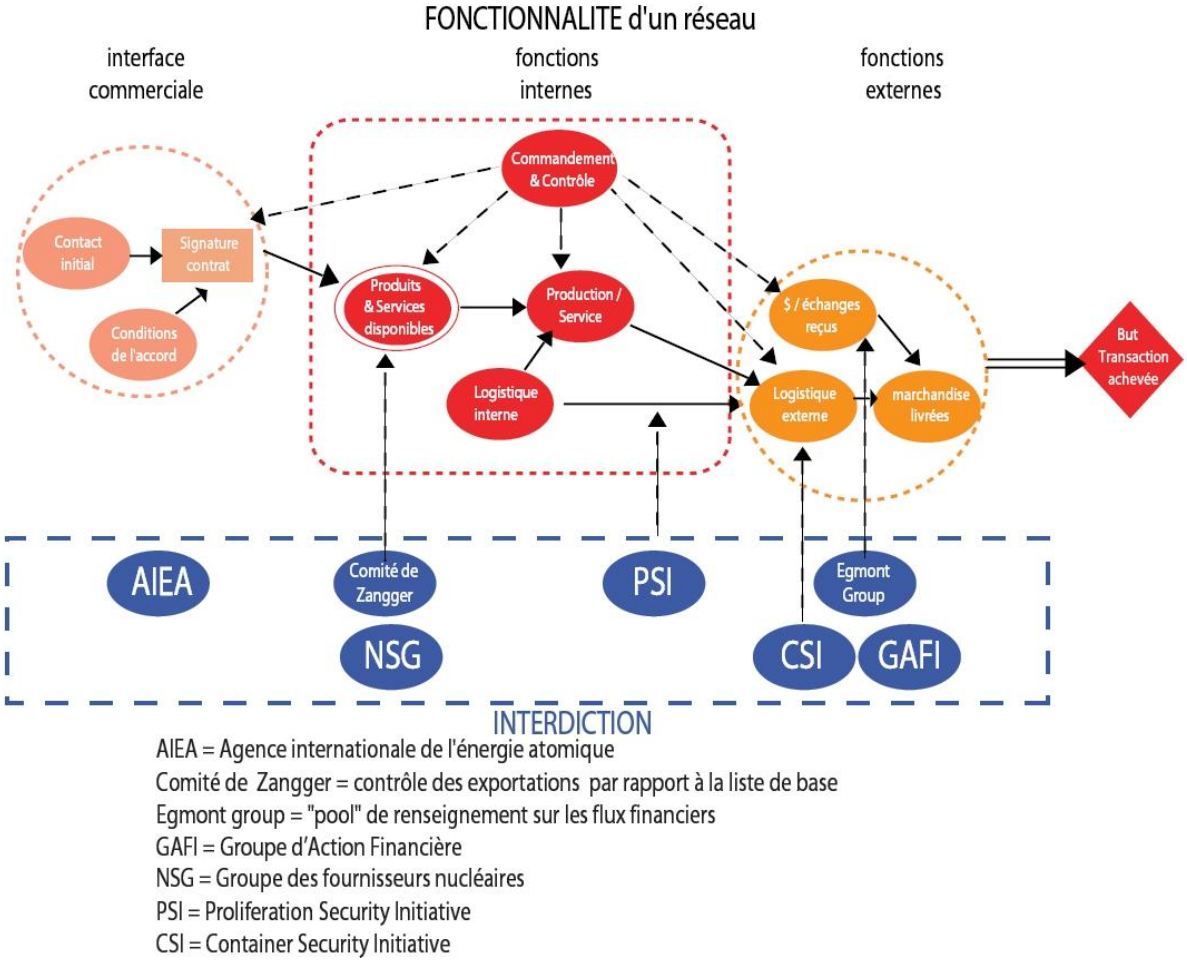



**Figure 9 : Organisation théorique de la lutte contre les trafics de prolifération**

## *2.1 – Le renseignement face aux réseaux de prolifération*

L'efficacité d'un système visant à neutraliser les activités des réseaux de prolifération repose en grande partie sur la capacité du renseignement non seulement à détecter les opérations réalisées par ces réseaux mais également sur la possibilité d'en préciser la structure et le mode opératoire.

Le travail de « cartographie » des réseaux repose d'abord sur la surveillance des flux, des individus et des sociétés permettant de détecter des activités proliférantes. A partir de là, l'objectif devrait être de rattacher ces bouts dans un ensemble cohérent. Par exemple, la surveillance d'un intermédiaire identifié du réseau Khan doit permettre de repérer les entreprises fournisseuses, les banques intermédiaires et éventuellement d'autres agents appartenant au réseau. Deux chausse-trappes semblent devoir être évitées dans cette démarche. D'une part, la tentation peut être forte de bloquer une opération du réseau avant d'avoir achevé la caractérisation de celui-ci, au risque de le voir se réorganiser et donc disparaître des acteurs dont la surveillance aurait pu permettre d'identifier un nœud clef[134]. *A contrario*, n'agir que lorsque le réseau est entièrement caractérisé peut conduire à laisser s'accomplir des transactions aux conséquences dramatiques en termes de dissémination de technologies nucléaires ou de missiles. Une intervention trop tardive peut par exemple conduire à l'obtention par un réseau de technologies clefs pour la réalisation d'un programme national. Or, les efforts en la matière dépendent de la capacité des services de renseignement à obtenir des informations complètes, précises et suffisamment fiables pour identifier le rôle de chaque acteur et la finalité des transactions. Vu la complexité potentielle des réseaux, en particulier la diversité en termes d'étendue et de spectre d'activité, de concentration fonctionnelle, voire les efforts de dissimulation qui peuvent être engagés, il ne fait aucun doute qu'une telle tâche est matériellement impossible. Un équilibre doit donc être trouvé entre la nécessité de parvenir à une cartographie la plus complète et détaillée possible et les impératifs d'intervention soit contre une transaction particulière, soit contre un acteur jugé suffisamment important pour que sa neutralisation affecte durablement les activités du réseau[135].

### *2.1.1 – L'organisation du renseignement pour la détection et l'investigation des réseaux de prolifération*

A la complexité des réseaux de prolifération doit répondre une variété de compétences en matière de renseignement permettant de traiter les aspects techniques, financiers, logistiques et humains des fonctionnements de ces organisations.

Qui plus est, d'un point de vue technique, les services de renseignement sont confrontés à la fois à la complexité et à la variété des domaines traités. Or, comme nous l'avons vu, pour échapper aux systèmes de contrôle, les réseaux se concentrent sur l'acquisition de biens élémentaires, qui pour en comprendre leur utilisation finale possible nécessite des compétences techniques importantes. Ainsi, dans le domaine de la prolifération plus que

[134] Les notes de la conférence « Terrorism Financing and State Responses in Comparative Perspective », Center for Contemporary Conflicrt, November 4-5, 2005, sont particulièrement intéressantes sur cette question.

[135] Le cas du démantèlement du réseau Khan procède de cette logique d'équilibre, les services américains de renseignement ayant vraisemblablement repoussé l'action contre le réseau afin de donner la possibilité d'agir le plus en profondeur possible.

dans d'autres – terrorisme, narcotrafic ou trafic d'armes –, le renseignement doit pouvoir s'appuyer sur des ressources propres ou extérieures pour traiter les aspects techniques.

En termes d'organisation du renseignement national, les trois grands pays occidentaux – États-Unis, Royaume Uni et France – disposent *a priori* d'outils similaires. En effet, chacun d'entre eux bénéficie d'un service de sécurité intérieur et d'une ou plusieurs organisations dédiées au renseignement extérieur. Chacune de ces organisations permet à la fois de suivre les activités d'éventuels réseaux sur son territoire et leurs ramifications à l'extérieur. Dans le domaine de la prolifération, elles ont en général développé des compétences propres en rassemblant des experts du renseignement, des spécialistes techniques et des connaisseurs des questions régionales. Ces compétences peuvent être complétées par l'intervention des services techniques des ministères de la Défense.

Ainsi, la France dispose-t-elle au sein de la Direction de la surveillance du territoire, de la Direction générale de la sécurité extérieure et de la Direction du renseignement militaire, d'organismes chargés des questions de prolifération qui bénéficient en outre du concours de la Délégation générale pour l'armement. La Direction nationale des recherches et enquêtes douanières, qui appartient au ministère des Finances, complète ce dispositif. Sa capacité d'investigation est renforcée par la possibilité pour les agents des douanes d'accéder aux documents commerciaux des sociétés, lui permettant de faire le lien entre les problématiques techniques et financières entourant les questions de prolifération[136]. Ainsi, les sections d'enquête des Douanes pourraient utilement participer à la traque des activités financières des réseaux, à partir du moment où celles-ci sont liées à des flux matériels[137]. En outre, les droits de visite domiciliaire, d'accès aux locaux et aux documents et de saisi qui leur sont accordés, constituent des atouts précieux dans l'effort de caractérisation des réseaux dans la mesure où ils permettent de recouper, de vérifier et de documenter des informations qui peuvent provenir de sources diverses.

Dans le domaine financier, en France, TRACFIN (traitement du renseignement et action contre les circuits financiers clandestins)[138] est chargé de recevoir les informations provenant du secteur privé et d'en assurer le recoupement avec les autres sources à sa disposition. L'organisme regroupe en effet, outre des fonctionnaires du ministère des Finances et des douanes, des agents des ministères de la Défense et de l'Intérieur. La cellule dispose en outre d'un droit de communication et d'échange de renseignements avec les services étrangers exerçant des compétences analogues. Pour autant, l'activité de TRACFIN se limite à la détection des opérations se déroulant sur le territoire national.

[136] http://www.douane.gouv.fr/page.asp ?id=501

[137] Notes d'entretiens.

[138] http://www.tracfin.minefi.gouv.fr/informations.htm

Côté américain en revanche, la création au sein du département du Trésor en 2004 de l'*Office of Terrorism and Financial Intelligence* (OTFI) s'inscrit dans une logique de lutte contre les flux financiers transnationaux[139]. En effet, au-delà des missions de renseignement, cet organisme dispose de pouvoirs juridiques dans le cadre de deux dispositions particulières :

- L'*Executive Order* 13382 du 28 juin 2005 (« *Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters* ») permet aux départements de la Justice, du Trésor et au département d'État d'interdire toute transaction entre les États-Unis et des personnes physiques ou morales participant à des activités de prolifération[140]. La section 5 autorise le département du Trésor à utiliser ces pouvoirs sans notification préalable aux personnes concernées.
- La section 311 du *Patriot Act* de 2001 permet au secrétaire au Trésor de couper du système économique américain une institution étrangère désignée comme étant préoccupante en matière de blanchiment (« *of primary money laundering concern* »).

Pour mener à bien ses missions, cet organisme dispose d'outils spécifiques visant à suivre les flux financiers internationaux. En particulier, l'obtention de données ciblées émanant de la société internationale de télécommunications financières interbancaires, SWIFT, semble faire partie de cet arsenal[141]. En outre, la concentration fonctionnelle réalisée au sein du département du Trésor des activités de sécurité financière permet à l'OTFI de mettre à contribution l'ensemble des services potentiellement concernés, y compris ceux menant des activités de renseignement ou de répression financière[142].

Si leurs domaines de compétence sont différents, les divers services de renseignement existants permettent donc aux États de disposer de capacités complémentaires de suivi et d'alerte concernant :

- Les individus et sociétés, opérant sur le territoire ou à l'extérieur, impliqués dans des activités de prolifération : l'activité de surveillance du territoire apparaît comme essentielle, elle permet en particulier de détecter les tentatives d'acquisition entreprises par les réseaux[143] mais également de cartographier les intermédiaires et les sociétés contactés ou utilisés à des fins proliférantes. Elle a aussi pour objectif de sensibiliser les acteurs privés aux questions liées à la prolifération. Cette démarche permet d'encourager la participation du secteur commercial au dispositif d'alerte et de veille en matière de prolifération. Celle-ci s'avère d'autant plus importante que les sociétés ciblées par les réseaux de prolifération peuvent être économiquement vulnérables, donc enclines à faire preuve de moins de rigueur vis-à-vis de leurs clients potentiels.
- Les programmes des acteurs proliférants : connaître la situation des efforts de développement des acteurs proliférants constitue un point de passage obligé pour combattre les réseaux qui les alimentent. En effet, une connaissance fine doit

[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

[141] « Prepared Remarks by Stuart Levey, Undersecretary for Terrorism and Financial Intelligence before the American Enterprise Institute », September 8, 2006.

[142] Entretien de l'auteur, novembre 2006.

[143] Entre 2003 et 2004, le MI-5 britannique indique avoir contribué au blocage de 30 tentatives d'acquisition menées par des « pays préoccupants ». http://www.mi5.gov.uk/output/Page161.html

permettre de déterminer dans quels domaines un réseau spécifique va rechercher une assistance extérieure. Pour autant, atteindre un tel niveau s'avère d'autant plus complexe que les programmes nucléaires ou de missiles sont souvent considérés comme stratégiques et font l'objet d'importantes mesures de sécurité. Le cas du programme biologique militaire irakien, dont Bagdad avait réussi à préserver le secret jusqu'en 1995 malgré les pouvoirs attribués à la commission spéciale des Nations Unies, montre les difficultés auxquelles peuvent être confrontées les services de renseignement. En définitive, il paraît possible d'obtenir au mieux une perspective générale sur l'avancement d'un programme, et éventuellement des informations précises sur certains de ses aspects.

➥ Les transferts matériels ou immatériels de technologies sensibles : le suivi des tentatives d'acquisitions, d'exportation ou de transport de technologies sensibles représente une part importante de l'activité des services de renseignement. En réalité, il convient de distinguer le renseignement concernant les opérations effectuées depuis le territoire national, dont l'objectif final peut être la neutralisation d'une branche ou d'agents travaillant au profit du réseau, et celui concernant les transactions à l'étranger qui participe à une entreprise de cartographie des activités du réseau. En l'occurrence, cette dernière peut avoir deux finalités, selon que les informations obtenues sont partagées avec des services alliés[144] ou utilisées pour compléter la connaissance nationale d'un réseau.

### *2.1.2 – L'Adaptation des outils de renseignement aux défis créés par les réseaux de prolifération*

Les dispositifs existants en Occident permettent donc, du moins pour ce qui concerne les territoires nationaux, d'assurer les missions de détection des flux matériels et des personnes impliquées dans des trafics de prolifération.

L'internationalisation du fonctionnement des organisations proliférantes ainsi que l'émergence de réseaux de réseaux soulèvent cependant la problématique de la coopération entre les services nationaux. En effet, si l'on peut estimer que, pour ce qui concerne le suivi des personnes et des transactions matérielles, les échanges de renseignement pratiqués entre les services occidentaux permettent d'atteindre un niveau satisfaisant de coopération[145], on peut s'interroger sur l'apport des services de renseignement d'États impliqués plus directement dans les trafics de prolifération. Ainsi, le degré de coopération du Pakistan dans la cartographie du réseau Khan, qui continue d'entretenir un réseau d'entreprises et d'intermédiaires pour son réseau d'acquisition[146], mérite *a minima* d'être relativisé. Il paraît en effet difficile d'imaginer qu'Islamabad livre l'ensemble des informations à sa disposition, sachant que certains des agents du réseau Khan agissent vraisemblablement encore à son profit. La coopération d'États servant de plates-formes

[144] Pour les alerter sur une activité ayant lieu sur leur territoire ou pour accroître la connaissance commune. Les États-Unis ont mis en place deux programmes destinés à vérifier l'utilisation finale des biens exportés vers des pays alliés : *golden sentry* et *blue lantern*, qui permettent de vérifier a priori la nature de l'utilisateur final ou de l'utilisation déclarée.
Voir pour illustration : http://www.dsca.mil/sc_conf_2002/Golden %20Sentry %20(Leon %20Yates).ppt

[145] Que ce soit sous forme bilatérale ou au niveau multilatéral au sein des régimes de contrôle, des initiatives d'interdiction ou encore de l'OTAN.

[146] Voir par exemple, http://www.armscontrolwonk.com/820/companies-and-organisations-of-proliferation-concern

pour certains trafics pose également problème du fait de l'importance économique des activités impliquées. Pour un pays comme Singapour, par exemple, la sauvegarde des intérêts économiques passe par la recherche d'un équilibre entre transparence vis-à-vis de ses alliés et protection de la confidentialité des activités des entreprises.

Par ailleurs, il est nécessaire de s'interroger sur la capacité de détection et de suivi des flux immatériels de technologies. En la matière, le développement d'outils permettant de suivre les échanges dématérialisés de manière globale reste encore balbutiant. Bien que les États-Unis aient engagé des efforts pour le contrôle de leurs propres entreprises[147], nous sommes encore loin de la mise en place d'une capacité de suivi mondiale (et de traitement) des données transitant par les réseaux téléphoniques et informatiques[148]. Pour autant, les progrès réalisés dans le domaine des technologies de l'information ont rendu plus simple l'interception des communications téléphoniques ou électroniques d'une personne identifiée. Dès lors, l'utilisation conjuguée des renseignements de sources humaines et d'origine technique doit permettre d'assurer cette mission au moins en partie.

Cette remarque s'applique d'ailleurs également aux flux financiers, en particulier pour ceux qui s'effectuent par voie électronique. Ainsi, il semble que dans le cas de la Banco Delta Asia, la transmission par SWIFT de données a permis de recouper des informations dont disposaient les services de renseignement américains. Il ne s'agissait pas, comme le montre le communiqué de la société[149] ainsi que les diverses interventions de responsables du département du Trésor, de suivre l'ensemble des données gérées par SWIFT mais bien d'accéder à des informations précises sur la base d'assignations juridiquement contraignantes.

Ainsi, dans le domaine de la surveillance des flux immatériels et financiers, les services de renseignement disposent potentiellement d'outils leur permettant de compléter les dispositifs établis pour le suivi des flux matériels et de personnes. Toutefois pour tirer parti de ces outils, les appareils de renseignement doivent pouvoir disposer de données fiables et précises provenant de sources humaines, qu'il s'agisse d'agents, de services étrangers ou encore du secteur privé.

### *2.1.3 – Améliorer l'efficacité des outils de renseignement face aux réseaux de prolifération*

Pour parvenir à améliorer l'efficacité des outils de renseignement dans la détection et la surveillance des réseaux de prolifération, deux voies devraient être privilégiées :

- Élargir et accroître la coopération internationale entre services de renseignement : il s'agit probablement de la tâche la plus difficile du fait des problèmes politiques, de sécurité voire économiques que les échanges de renseignement peuvent soulever. Une première étape pourrait consister à étendre les échanges entre les services au

[147] B. Gruselle, « Missiles de croisière et stratégies d'anti-accès », Etude FRS, décembre 2005, p. 50.

[148] Pour autant, la mise sur pied d'une telle capacité n'est techniquement pas irréalisable. Pour ce qui concerne Internet, par exemple, le système repose sur quelques milliers de stations relais (des routeurs) dirigeant le trafic d'information entre les serveurs reliés au réseau. L'implantation de systèmes d'interception au niveau de ces routeurs peut permettre en théorie de suivre les échanges sur la toile. On notera toutefois que la question centrale concerne davantage le traitement des informations obtenues ainsi.
Voir, http://computer.howstuffworks.com/router.htm/printable.

[149] http://www.swift.com/index.cfm ?item_id=59897

sein des grands régimes multilatéraux aux questions de suivi et de contrôle des flux matériels, immatériels et financiers. En mettant sur pied en 2002 un forum d'échange dédié aux experts du contrôle, le régime de contrôle des technologies de missiles (MTCR) s'inscrit dans une logique de renforcement du dialogue sur les méthodes des réseaux de prolifération voire le traitement de cas d'espèce[150]. En outre, ce type de forum contribue à créer des liens entre experts et à faciliter effectivement les échanges bilatéraux. Dans le domaine financier, le groupe Egmont, créé en 1995 pour coordonner les organisations de renseignement, comprend également un groupe de travail à caractère opérationnel – il inclut en particulier les services de Singapour, des Émirats Arabes Unis ou encore de Malaisie – qui participe de la même logique[151]. Le lancement de la *proliferation security initiative* (PSI) et, surtout de la *container security initiative* (CSI) a, semble-t-il, contribué à accroître les échanges entre les services des pays qui y participent, mais surtout entre ces services et ceux des États-Unis[152]. De façon générale, le développement de la coopération et de l'assistance douanière bilatérale constitue un moyen efficace de renforcer les échanges de renseignement à caractère opérationnel entre les pays impliqués. Elles s'avèrent particulièrement utiles pour développer ceux-ci avec des pays jouant un rôle central dans le fonctionnement logistique des réseaux, comme par exemple les pays de transbordement.

➥ Accroître l'implication du secteur privé dans la détection des activités des réseaux : les sociétés industrielles ou de service, les établissements bancaires ou financiers ou encore les intermédiaires jouent des rôles importants dans le fonctionnement et l'approvisionnement des réseaux de prolifération. Pour la plus grande partie d'entre eux, leur implication ne repose que sur des intérêts économiques et, le plus souvent, sur une méconnaissance de leur client et/ou de l'utilisation possible des biens, services ou technologies qu'ils sont amenés à fournir. Dès lors, il s'avère essentiel d'impliquer plus largement ces acteurs dans les efforts étatiques de lutte contre les réseaux de prolifération. En termes de renseignement, il s'agit en particulier d'engager les sociétés à rapporter toute opération suspecte dans laquelle ces entreprises pourraient être impliquées. En France, un tel devoir existe d'ores et déjà pour les établissements bancaires et financiers dans le cadre de la lutte contre le blanchiment, mais son extension au reste du secteur commercial est encore limitée. Plusieurs raisons peuvent être avancées pour l'expliquer :

  ⇨ Le nombre d'entreprises concernées : comme nous l'avons vu, les réseaux de prolifération vont être de plus en plus amenés à tenter d'acquérir des composants élémentaires, élargissant la palette des activités techniques concernées et donc, le nombre de sociétés susceptibles d'être ciblées. Pour obtenir l'assistance de celles-ci une démarche de sensibilisation et d'information doit être entreprise par les administrations chargées du contrôle des biens à double usage. Or, en l'absence de processus formel d'enregistrement administratif[153], dresser une cartographie

[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] Pour mémoire, les ports ayant signé avec les États-Unis des accords CSI acceptent l'implantation de cellules douanières américaines qui peuvent demander le contrôle d'un containeur donné sur la base d'informations nationales. Voir par exemple, Département d'État, « Container Security Initiative Now Operational in Singapore », March 18, 2003.

[153] Comme celui qui autorise les sociétés à produire ou commercer des matériels de guerre.

précise des sociétés produisant des biens à double usage s'avère quasiment impossible.

⇨ La taille et la situation économique des sociétés : les plus petites sociétés constituent une cible particulièrement attractive pour les réseaux et leurs agents dans la mesure où elles s'avèrent souvent dépendantes pour leur survie et/ou leur indépendance économique d'un nombre limité d'affaires. Cette dépendance les conduit à être moins attentives à la nature du client, à la sensibilité du bien concerné ou encore à la mise en place de circuits d'acheminement inhabituels. Cette tendance est encore renforcée par l'absence ou la légèreté des peines et amendes éventuellement encourues en cas de contournement des législations de contrôle en vigueur. L'application publique de sanctions lourdes possède non seulement un rôle dissuasif mais également une vertu de sensibilisation[154]. En la matière, l'adoption et l'application stricte de législations de type « attrape-tout » semblent constituer la meilleure solution dans la mesure où il s'agit de faire porter la responsabilité aux entreprises de vérifier que le bien qu'elle souhaite vendre et/ou son destinataire final ne sont pas sensibles[155].

Les efforts d'amélioration de l'outil de renseignement contre les réseaux de prolifération devraient donc porter sur le développement d'une relation étroite entre les services et les sociétés sensibles de petite taille. La première étape nécessaire pour y parvenir est de dresser et de maintenir à jour une liste exhaustive des sociétés potentiellement concernées. L'introduction de dispositions de type attrape-tout dans la législation nationale peut faciliter ce processus, en amenant les sociétés à se rapprocher des services officiels. Il conviendrait ensuite de définir la nature des échanges entre les sociétés et les services de renseignement. Si l'on prend l'exemple de TRACFIN, la cellule reçoit les déclarations de soupçon mais assure également un retour vers le déclarant sous deux formes : une information sur le traitement de sa déclaration et des actions de formation, d'information et de sensibilisation ciblées ou non. De même, le département américain du Trésor assure une mission d'information auprès des établissements financiers qui complète les actions de publicité autour des cas ayant fait l'objet de mesures répressives[156]. In fine, il paraît essentiel que cet effort permette de construire un dialogue entre les acteurs privés et les services de renseignement.

### *2.2 – La neutralisation des réseaux : moyens, limites et perspectives*

Parvenir à neutraliser durablement les réseaux de prolifération constitue le principal objectif en matière de lutte contre ce phénomène. En amont de cet effort se trouve la possibilité grâce au renseignement de disposer d'une cartographie même imparfaite de ces réseaux (structure, organisation fonctionnelle). Il est possible de concevoir plusieurs types d'outils permettant de parvenir à ce résultat : outils financiers, économiques, policiers ou encore juridiques. Mais, du fait de l'assise internationale des réseaux de prolifération, ils ne peuvent fonctionner que dans la mesure où ils font l'objet d'une adoption la plus large possible par les États. Il paraît donc essentiel dans un premier

[154] La publicité qui peut être faite autour des affaires de répression financière ou de contrôle des exportations, que pratique l'administration américaine, permet en particulier de faire prendre conscience aux secteurs concernés que le contournement des règles établies ou la légèreté dont ils font preuve vis-à-vis de la connaissance de leur client a un impact économique non négligeable. Entretiens à Washington, novembre 2006.

[155] Nous reviendrons sur les clauses de type attrape-tout dans la suite du document.

[156] Entretiens de l'auteur, novembre 2006.

temps de récapituler les fondements juridiques internationaux existants qui pourraient faciliter cette harmonisation.

### *2.2.1 – Les fondements internationaux en matière de lutte contre les réseaux de prolifération*

En adoptant le 28 avril 2004 la résolution 1540, le Conseil de sécurité des Nations Unies a posé les fondements de la lutte internationale contre les réseaux de prolifération en s'appuyant sur le chapitre VII de la Chartre. Dans ses considérants, la résolution pose le problème en ces termes : « *gravement préoccupé par la menace que constitue le trafic d'armes nucléaires, chimiques ou biologiques et de leurs vecteurs, ainsi que des* ***éléments connexes***[157]*, qui ajoute une dimension nouvelle à la question de la prolifération de ces armes et fait également peser une menace sur la paix et la stabilité internationales* ». Cette résolution a donc pour objet, entre autres choses, de réduire les trafics de biens, de technologies et de savoir-faire dans les domaines nucléaires et des missiles. Elle insiste également sur la nécessité d'empêcher des acteurs non étatiques d'accéder à ce type d'armes.

Le Conseil de sécurité impose aux membres des Nations Unies plusieurs types de mesures, qui peuvent avoir un impact direct sur le fonctionnement des réseaux :

1. L'interdiction des activités illégales d'intermédiation pour les armes, vecteurs et éléments connexes : c'est l'objet en particulier du point c) de l'article 3 qui impose que soient prises les mesures permettant de détecter, dissuader, prévenir et combattre l'intermédiation.
2. Le contrôle des utilisateurs finaux : le point d) de l'article porte essentiellement sur le contrôle du transit et du transbordement, mais il oblige également les États à établir des moyens de contrôler la nature de l'utilisateur final.
3. Le contrôle des services et des fonds pour les opérations d'exportation : ce même point impose également aux États de contrôler « *la fourniture de fonds ou de services – financement ou transport par exemple – se rapportant aux opérations d'exportation ou de transbordement qui contribueraient à la prolifération* ».

On peut regretter toutefois, qu'en matière de service la résolution 1540 se contente de demander un contrôle des services liés aux exportations. En effet, certains réseaux utilisent des établissements bancaires et financiers intermédiaires sans qu'ils soient impliqués, sur le territoire sur lequel ils opèrent, dans des exportations.

Une autre résolution du Conseil de sécurité comble ce vide, mais elle ne le fait que dans le cas particulier de la Corée du Nord. En effet, la résolution 1695 du 15 juillet 2006 cible directement les activités de fourniture et d'acquisition de Pyongyang. Le paragraphe 4 exige en particulier des États membres qu'ils exercent une vigilance accrue afin de prévenir l'acquisition auprès de la Corée du Nord de missiles, de technologies et de biens liés aux missiles et aux armes de destruction massive. Il ajoute que cet effort

[157] Les caractères gras ont été rajoutés par l'auteur. La résolution définie les éléments connexes ainsi : matières, équipements et technologies couverts par les traités et les arrangements multilatéraux pertinents, ou figurant sur les listes de contrôle nationales, susceptibles d'être utilisés aux fins de la conception, de la mise au point, de la fabrication ou de l'utilisation d'armes nucléaires, chimiques ou biologiques ou de leurs vecteurs.

doit également s'appliquer à **tout transfert financier** ayant une relation avec les programmes non conventionnels nord-coréens[158].

Le cadre juridique international, fixé par la résolution 1540, mérite d'être amélioré, en particulier autour des lignes fixées par le texte de la résolution concernant les programmes non conventionnels nord-coréens. Toutefois, même si le Conseil de sécurité parvenait à un texte plus abouti, son application universelle demeurerait improbable. En revanche, l'extension progressive à des États sources[159] des principes de lutte contre les réseaux de prolifération paraît envisageable au travers d'initiatives *ad hoc* ou de groupes multi-latéraux. Ainsi, l'extension de la *Proliferation Security Initiative* à une coopération entre les polices mérite d'être explorée[160]. Elle aurait pour objet de faciliter les enquêtes nationales menées sur des personnes ou des organisations liées aux réseaux, par l'échange d'information et la facilitation des mesures d'extradition.

Pour autant, il convient de souligner que le domaine d'application de la résolution 1540 reste très limité. En effet, il se limite à criminaliser la prolifération des armes non conventionnelles conduite par des acteurs non étatiques[161]. En conséquence, et même si le texte est à dessin ambigu concernant la prolifération des États, son extension à ce cas paraît politiquement improbable, dans la mesure où certains pays poursuivent légalement des activités de développement d'armes nucléaires et *a fortiori* de missiles.

La résolution 1718 du 14 octobre 2006[162], votée suite à l'essai nord-coréen du 9 octobre 2006, pourrait devenir un standard en matière de lutte contre les réseaux de prolifération. Outre le gel des avoirs nord-coréens, elle dispose dans l'article 8.d que les États doivent empêcher leurs ressortissants et les personnes agissant sur leur territoire de fournir une aide financière à toute personne ou entité impliquée dans les programmes de missiles ou nucléaires de la Corée du Nord. Elle décrète également dans l'article 8.f que tout fret entrant ou sortant du territoire devra être soumise à une fouille. L'application de cette résolution, au-delà de sa vertu d'exemple pour de futurs ou actuels dossiers de prolifération, pourrait permettre d'assainir les méthodes de certaines sociétés de service qui soutiennent aujourd'hui directement le fonctionnement des réseaux, qu'il s'agisse des établissements bancaires mais aussi des professions du transport et de l'affrètement[163]. En particulier, l'application de cette résolution pourrait conduire les sociétés concernées à exercer une vigilance accrue vis-à-vis de la nature et des activités de leurs clients et éventuellement à renforcer le dialogue entre le secteur privé et les services et agences chargées de la lutte contre la prolifération[164].

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

[159] On désigne ainsi les États dans lesquels sont implantés des sociétés dont les réseaux de prolifération tentent d'acquérir des biens ou technologies. Par extension, on y ajoute les paradis fiscaux, les États de pavillon de complaisance et les pays servant de plaque tournante aux trafics.

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

[161] Voir les articles 1 et 2.

[162] Sous chapitre VII.

[163] Entretiens de l'auteur, novembre 2006.

[164] Cf. §2.1.3.

### *2.2.2 – Les outils de lutte contre les réseaux de prolifération*

La mise en place d'organisations multilatérales doit permettre de coordonner les politiques des États sources dans la lutte contre les réseaux. De tels outils doivent donc inclure à la fois des États producteurs de technologies mais également des pays abritant des activités de service[165] susceptibles d'être exploitées par les organisations se livrant au commerce d'armes de destruction massive.

Le rôle de ces outils est donc de concevoir les moyens de neutraliser durablement les fonctions clefs les plus fragiles des réseaux, ces dernières ayant été identifiées au préalable par les efforts en matière de renseignement. Deux remarques s'imposent :

1. La partie interne des réseaux, c'est-à-dire celle qui fonctionne sans contact avec l'extérieur paraît ne pouvoir être démantelée que par le biais d'une action politique visant la volonté de l'acteur proliférant – ou des États qui le soutiennent – de poursuivre ses activités. Ainsi, dans le cas du réseau Khan, la neutralisation de la fonction technique a nécessité l'intervention des autorités pakistanaises.
2. La neutralisation d'une fonction n'est pas toujours suffisante pour obtenir le démantèlement du réseau. Si cela est le cas pour les structures en étoile, il faut mettre en place des stratégies particulières pour les réseaux cycliques ou informels. Dans ces derniers cas, le démantèlement sera effectivement obtenu soit si toutes les fonctions sont neutralisées, soit si toutes les connexions entre elles sont dissoutes[166].

Mettre un terme aux activités des réseaux de prolifération doit en conséquence s'appuyer sur un ensemble de mesures complémentaires visant à atteindre l'ensemble des fonctions et des liens opérationnels au sein de ceux-ci. Il s'agit en particulier :

- d'empêcher les mouvements financiers entre les banques dépendantes du réseau, les banques intermédiaires et les banques locales ;
- de neutraliser les intermédiaires, agents et sociétés écrans opérants au profit du réseau ;
- d'entraver la production et les mouvements de biens réalisés au profit du réseau[167].

Même si son action est aujourd'hui concentrée sur le blanchiment d'argent et le financement du terrorisme, le Groupe d'action financière internationale (GAFI) constitue le cadre le plus adapté pour coordonner la lutte contre le financement de la prolifération. En l'occurrence, l'adoption de la résolution 1540 permettrait effectivement d'étendre son domaine d'action à cette catégorie. Créé en 1989 par le G-7, le GAFI comprend aujourd'hui 33 pays membres[168], ce corps étant complété par des pays observateurs et par l'existence de forums régionaux – par exemple un groupe Asie–Pacifique auquel la Chine appartient – et la participation d'agences ou d'organisations internationales. A travers 40 recommandations, le GAFI offre le cadre d'une action internationale

[165] Financement, transport/affrètement, transbordement, intermédiation.

[166] Alexander H. Montgomery, « Ringing in Proliferation », op. cit., p. 170.

[167] Ce point sera développé dans le chapitre suivant.

[168] Pour la liste des membres voir http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html#FATF_Members

concertée sur le financement des trafics de prolifération, ce d'autant que ces recommandations sont reconnues par la banque mondiale et le Fonds Monétaire International[169].

Les recommandations du GAFI portent essentiellement sur deux domaines.

En premier lieu, la nécessité pour les États de disposer d'un cadre juridique permettant de poursuivre les personnes physiques ou morales impliquées dans des activités de blanchiment. Il doit prévoir des mesures provisoires (gel ou saisie) ou définitives (confiscation) visant les biens blanchis, les produits découlant du blanchiment ainsi que les instruments utilisés pour cette infraction. Une telle recommandation pourrait être étendue à la répression des activités financières des réseaux de prolifération comme elle l'a été à celle des groupes terroristes.

Par ailleurs, le GAFI propose plusieurs voies pour renforcer le rôle des institutions financières dans la lutte contre le blanchiment et le financement du terrorisme qui pourraient être intéressantes en matière de financement de la prolifération. Il s'agit en particulier d'obliger les établissements financiers à identifier et à vérifier les activités de leurs clients et des établissements bancaires avec lesquels ils se mettent en relation. En cas de doute, ils sont invités à décliner la clientèle de la personne ou la création de liens avec la banque. Par ailleurs, les établissements bancaires sont invités à être particulièrement vigilants sur les mouvements de capitaux par voie électronique ainsi qu'aux opérations inhabituelles. Le GAFI invite également les États à mettre en place un système de déclaration de toutes les transactions nationales et internationales en espèces supérieures à un certain montant. Une telle mesure frapperait directement les réseaux de prolifération qui doivent souvent réintroduire dans le système bancaire des fonds en espèces.

L'extension des recommandations du Groupe d'action financière international au financement des réseaux de prolifération constitue une piste intéressante pour créer le premier pilier de l'action contre ceux-ci. L'existence de deux résolutions du Conseil de sécurité concernant la criminalisation de la prolifération pourrait du reste constituer la base d'une telle extension. Il convient toutefois de s'interroger sur la faisabilité d'une telle initiative, sachant que certains pays liés au GAFI – c'est le cas de la Chine ou encore du Pakistan – participent aujourd'hui à des activités de prolifération et pourraient donc être victimes de l'extension des recommandations. Qui plus est, le cadre d'application de la résolution 1540 se limite aujourd'hui au cas des acteurs non étatiques. Son extension au cas de la prolifération par les États soulève des problèmes délicats, en particulier dans le domaine des missiles pour lequel il n'existe aucun traité ou convention d'interdiction. Toutefois, dans la mesure où ces États se reposent pour leurs acquisitions sur des structures ou des personnes qui ne leur sont pas directement liées, il paraît envisageable de cibler celles-ci sans remettre en question les droits des États. En d'autres termes, il paraît possible d'étendre le rôle du GAFI à la lutte contre la partie souterraine de la prolifération.

En complément de la mise en place d'une politique internationale de lutte contre le financement de la prolifération, des mesures visant les acteurs économiques utilisés par les réseaux doivent être envisagées. Elles doivent en particulier permettre de neutraliser les intermédiaires utilisés par les réseaux pour conduire leur contact avec les entreprises ciblées. Dans ce domaine, si les groupes de fournisseurs – MTCR, NSG ou Wassenaar –

[169] 40 recommandations du GAFI, voir http://www.fatf-gafi.org/dataoecd/7/55/34850891.PDF

semblent avoir engagé des efforts d'échange et de coordination[170], les États restent encore relativement inactifs. A l'exception des États-Unis qui ont introduit en 1996 des dispositions concernant les intermédiaires dans la loi sur le contrôle des exportations d'armes[171], peu de pays possèdent des instruments juridiques visant les courtiers[172]. De son côté pourtant, le Conseil de l'Union Européenne a adopté en 2003 une position commune sur le contrôle des intermédiaires en armement[173]. Il s'agit, dans les deux cas, de :

- Recenser les courtiers opérants sur le territoire concerné. La mise en place d'un système d'autorisation d'activité est parfois envisagée comme un moyen de mieux contrôler les opérateurs.
- Obliger les intermédiaires à obtenir une autorisation préalable pour chacune des opérations dans laquelle ils s'engagent.
- Établir un système juridique punissant les activités d'intermédiation non autorisées.

Étant données la nature transnationale des activités des intermédiaires et leur mobilité géographique, il apparaît en première analyse que seule une internationalisation du contrôle de cette profession est susceptible d'apporter une réponse à son implication dans la prolifération. Bien entendu, il est très improbable de parvenir à un tel état final. Pour autant, comme nous l'avons vu, les courtiers ne peuvent pas profiter à plein de cette liberté et doivent disposer d'attaches locales pour pouvoir mener à bien leurs opérations. Qui plus est, cette profession se caractérise par la diversité des affaires traitées, leur activité étant essentiellement guidée par la demande des clients. Paradoxalement, on peut estimer que confrontés à un choix entre leur implantation locale et une partie de leurs affaires, la plupart des intermédiaires abandonneraient les activités illicites. Ainsi, la mise en place par des ensembles géographiques de pays de lois cohérentes sur le courtage des armes non conventionnelles conduirait vraisemblablement à réduire le rôle des intermédiaires commerciaux dans le fonctionnement des réseaux. Elles auraient aussi un effet pour les agents opérant exclusivement au profit des réseaux de prolifération en rendant leur activité illégale. Il paraît donc essentiel que les États sources, en particulier occidentaux, se dotent sans attendre de législations visant à encadrer l'activité d'intermédiation à la fois dans le domaine des systèmes complets mais également des biens à double usage qui y sont associés, conformément d'ailleurs à la résolution 1540.

En conclusion, si dans le domaine financier les outils multilatéraux semblent pouvoir être utilisés pour mieux lutter contre les réseaux de prolifération, il paraît nécessaire d'améliorer ceux portant sur la neutralisation des intermédiaires et agents agissant pour le compte de ces réseaux. Les États occidentaux devraient en particulier adopter au plus vite des mesures légales permettant d'encadrer les activités des courtiers dans le domaine des armes de destruction massive et des biens et technologies associés.

[170] Voir le communiqué de la 20ème réunion plénière du régime de contrôle des technologies de missiles : http://www.mtcr.info/english/press/madrid.html

[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] On notera que la loi américaine rend l'autorisation de courtage obligatoire pour tous les citoyens des États-Unis quel que soit leur pays d'implantation.

[173] Conseil de l'UE, « Position sur le contrôle des intermédiaires en armement », 2003/468/CFSP, 23 juin 2003.

### *2.2.3 – Quelles évolutions possibles pour le contrôle des flux de biens et de technologies ?*

La capacité des États à interdire effectivement l'exportation depuis leur territoire de biens ou de technologies convoités par eux constitue probablement l'un des principaux outils pour neutraliser durablement l'activité des réseaux. Si, par exemple, les autorités malaisiennes avaient été capables d'empêcher la livraison des pièces fabriquées par la société SCOPE au réseau Khan, celui-ci aurait probablement rencontré d'importantes difficultés pour honorer la commande libyenne. En effet, comme nous l'avons remarqué, les réseaux, de fournisseurs comme d'acquisition, dépendent de fournisseurs industriels extérieurs pour parvenir à leur fin.

Le contrôle des flux matériels et immatériels repose dans la plupart des États sur un ensemble cohérent de moyens et de mesures[174] qui s'appuient sur l'existence **de listes de biens et de technologies** pour lesquels l'exportation et le transit sont en général soumis à l'obtention d'autorisations préalables délivrées par les autorités. L'élaboration de listes efficaces constitue en conséquence un enjeu central en termes de contrôle des flux.

C'est le cas en particulier pour celles qui concernent les biens à double usage. En effet, les systèmes complets et leurs principaux composants sont en général relativement bien contrôlés. Dans la mesure où il n'existe qu'un petit nombre d'industriels capables de les assembler ou de les produire, ces derniers comme les autorités nationales sont conscients de leur sensibilité.

*A contrario*, l'élaboration et surtout la mise à jour des listes des biens à double usage s'avèrent des tâches difficiles compte tenu de l'évolution constante des technologies[175]. Le principal écueil d'une approche reposant uniquement sur l'existence de listes se situe au niveau de l'application du contrôle. Pour un pays possédant des ressources administratives limitées[176], le poids de la gestion des demandes d'exportation ou de transit de biens à double usage peut devenir tel qu'il entraîne des disfonctionnements de leur traitement : retards, analyses superficielles, erreurs, etc.. De la même façon, les industriels, mal ou pas informés et déresponsabilisés, seront enclins à effectuer des demandes incomplètes ou inexploitables.

Plusieurs alternatives sont envisageables afin d'améliorer le contrôle des biens à double usage et d'éviter les problèmes d'une approche fondée uniquement sur l'utilisation de listes.

La mise en place de clauses « attrape-tout » répond en partie à cette problématique. Il s'agit non plus de juger de la sensibilité intrinsèque d'un bien mais de celle du destinataire et de l'utilisation possible qu'il pourrait en faire[177]. Les clauses attrape-tout rendent en outre obligatoire pour les exportateurs d'informer les autorités de contrôle en cas de soupçon sur la finalité du bien ou la nature de l'utilisateur final, contribuant ainsi – à

[174] En particulier des contrôles physiques ou documentaires pouvant avoir lieu avant ou au moment de l'exportation. Les États-Unis pratiquent également le contrôle après exportation et le suivi des biens exportés.

[175] Il suffit pour s'en convaincre de regarder les listes de biens élaborés par l'arrangement de Wassenaar.

[176] Ceux précisément dont on peut souhaiter qu'ils soient vigilants en termes de contrôle dans la mesure où ils sont les cibles principales des réseaux.

[177] Irina Albrecht, « Catch-all controls », paper prepared for the International Control Conference, London, 2004.

l'instar du contrôle des flux financiers – à la responsabilisation des sociétés[178]. De fait, on ne peut concevoir une telle responsabilisation qu'avec une contrepartie en termes d'information et de formation des sociétés. Dans ce domaine, outre la formation des cadres des entreprises, il paraît également utile de publier sur une base périodique un rapport de violation des règles de contrôle[179].

Outre l'adoption de clauses « attrape-tout », la possibilité d'élaborer des listes de destinataires finaux devrait être envisagée. De tels documents, malgré les difficultés politiques qui peuvent entourer leur création, possèdent un réel intérêt dans le cadre de la lutte contre les réseaux de prolifération, à partir du moment où les travaux de renseignement en amont ont permis de cartographier la structure de ceux-ci. Ce d'autant que l'élaboration de ce type de document peut tout à fait être envisagée au sein de groupes multinationaux[180] afin de mieux coordonner les efforts d'un groupe de pays.

La mise en place d'une politique globale de limitation volontaire de la dissémination de technologies proliférantes mérite d'être explorée. En 2004, le président Bush avait proposé dans le cadre d'un discours à la *National Defense University* d'interdire aux États ne les possédant pas d'acquérir les technologies d'enrichissement et de retraitement[181]. Malgré les polémiques qu'a pu engendrer cette proposition, nous avons montré que la dissémination des technologies facilite l'action des réseaux de prolifération et par conséquent la limiter aurait vraisemblablement comme effet de rendre leur tâche plus difficile. Cette remarque vaut autant pour les technologies liées au cycle du combustible[182] qu'à celles utilisées, par exemple, dans le domaine des lanceurs spatiaux. Ce type de proposition aurait le mérite de réduire le risque de voir apparaître de nouveaux réseaux structurés capables de fournir un produit complet. Mais cette proposition ne peut valoir que si elle s'accompagne d'une internationalisation – et d'un durcissement –des mesures de contrôle sur les composants élémentaires en particulier à double usage.

[178] Ibid. Pour un exemple de déclaration de soupçon voir : https ://www.bis.doc.gov/forms/eeleadsntips.html

[179] Le bureau de la sécurité industrielle du département du Commerce américain, en charge du contrôle des exportations de biens à double usage, publie annuellement un document de ce type. Pour l'année 2006, voir http://www.bis.doc.gov/ComplianceAndEnforcement/Majorcaselist.pdf

[180] Par exemple des groupes de fournisseurs : MTCR, NSG.

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

[182] Certains États ont d'ores et déjà annoncé leur volonté de reprendre ou de débuter des activités d'enrichissement à finalité civile.

### *2.3 – L'action armée et l'endiguement des flux de prolifération*

Les outils et méthodes décrits précédemment visent essentiellement à neutraliser un réseau dans son ensemble, à partir du moment où sa structure et son organisation présentent des vulnérabilités suffisantes pour être exploitées. De façon pratique, dans le cas de réseaux étatiques, une partie de la structure s'avère impossible à neutraliser[183]. On peut certes s'attacher à neutraliser ses agents, à ralentir ses flux financiers ou encore à rendre difficile son accès aux fournisseurs. Mais tout porte à croire que ces réseaux pourront continuer à fonctionner, d'abord dans un mode dégradé puis éventuellement normalement, en se tournant vers des fournisseurs ou intermédiaires moins regardant localisés dans des États plus laxistes en matière de contrôle.

Dès lors, vu le risque considérable qu'engendre l'accès de ces réseaux aux biens et technologies qu'ils recherchent, nos politiques doivent permettre d'intervenir de façon ciblée sur des transactions spécifiques afin de les empêcher. En outre, il paraît nécessaire de s'interroger sur la pertinence d'autres solutions faisant appel à des moyens militaires et susceptibles d'affecter la partie interne de ces réseaux, y compris de façon indirecte.

Le lancement de l'initiative de sécurité sur la prolifération (PSI) en mai 2003 a créé le cadre nécessaire pour une coopération internationale entre les forces armées des pays participants afin de permettre l'interception et la fouille de cargos suspects. Le principal intérêt de cette initiative, malgré ses faiblesses juridiques[184], est de permettre d'arrêter les flux matériels de biens proliférants alors qu'ils ne sont plus dans la zone de responsabilité des pays membres et en particulier dans des espaces internationaux. Ainsi, elle permet en partie de répondre à la faiblesse de certains systèmes de contrôle nationaux. Mais, pour fonctionner, la PSI nécessite que soit accompli le travail de cartographie déjà évoqué dans les chapitres précédents. Comme l'a rappelé le président Bush en février 2004 lors d'un discours à la *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.* »

C'est donc le travail de renseignement en amont qui a permis l'arraisonnement du navire allemand *BBC China* et des pièces fabriquées par SCOPE au profit du réseau en octobre 2003[185], conduisant par ricochet à la mise en lumière des activités de A. Q. Khan et au démantèlement – au moins en partie – du réseau qu'il dirigeait.

[183] Cf. § 2.2.2 du présent document.

[184] B. Gruselle, « Missiles de croisière et stratégies d'anti-accès », op. cit., p. 48.

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

Les opérations d'interdiction paraissent servir deux finalités en termes de lutte contre les réseaux de prolifération :

- Empêcher ponctuellement la livraison d'un bien : même si l'enquête sur le réseau n'est pas terminée, il pourra être essentiel dans certains cas spécifiques d'interdire l'acquisition d'un bien. Cela peut s'appliquer par exemple à la livraison de composants clefs pour la production du système considéré ou encore à la volonté de neutraliser une partie de la filière.
- Conclure une enquête afin d'exposer l'ensemble d'un réseau : il peut être utile dans une optique de diplomatie publique de conclure une enquête sur un réseau par une interdiction. Le cas du *BBC China* illustre ce principe, servant tout à la fois de préambule au démantèlement du réseau Khan[186] mais également de message dans le cadre de la négociation entre la Libye, les États-Unis et le Royaume Uni.

Malgré ses succès, l'initiative de sécurité sur la prolifération (PSI) demeure un édifice fragile. En particulier, ne s'agissant pas d'une organisation internationale, elle reste tributaire d'éventuels changements politiques à la tête des États qui y participent[187]. Il suffirait sans doute que les États-Unis décident d'abandonner progressivement leur implication pour que l'initiative se délite. Sans en venir à des solutions d'institutionnalisation, qui à long terme auraient vraisemblablement pour effet la perte d'efficacité du système, il conviendrait d'inscrire la PSI dans un cadre plus formel. L'une des solutions pourrait être d'en faire acter les grands principes par une résolution du Conseil de sécurité des Nations Unies qui viendrait compléter la 1540[188]. Même si cela pourrait réduire la marge de manœuvre des pays membres de la PSI, du moins le principe de la lutte contre les réseaux de prolifération serait inscrit dans un texte de portée universelle.

Dans l'immédiat, l'amélioration des volets militaires et politiques de la PSI passe sans doute par une extension de son champ d'application. En effet, les opérations de fouille et de saisie ne sont possibles que dans un cadre très strict : autorisation de l'État d'immatriculation du véhicule[189] ou dans le cadre des attributions légales des États dans leur espace territorial. Cela pose le problème de l'interdiction des véhicules immatriculés dans un État non coopératif et circulant dans des espaces internationaux. Il existe deux possibilités pour améliorer le dispositif :

- Sur une base *ad hoc* – i.e. une résolution spécifique du Conseil de sécurité – autoriser les pays membres des Nations Unies à intercepter des véhicules appartenant à un État dans les eaux internationales. En réalité, il s'agirait plutôt dans ce cas de la préparation d'une résolution portant sur un problème de prolifération spécifique – comme ce fût le cas de la résolution 1718 sur la Corée du Nord ou d'une éventuelle résolution sur l'Iran – d'autoriser les États à fouiller un navire ou un appareil aérien appartenant au pays concerné. On peut toutefois s'interroger sur la faisabilité d'une démarche de ce type au regard des réticences de la Chine et de la Russie à adopter des sanctions sur des dossiers de prolifération.

[186] Insistons de nouveau sur le fait que ce démantèlement n'est peut être ni définitif, ni complet. Toutefois il constitue *a priori* une réussite considérable des efforts de lutte contre les réseaux.

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

[188] Cf. supra pour les principes d'extension de la résolution 1540.

[189] En général, sur la base d'un accord bilatéral.

➥ La fouille systématique et si possible complète de tout véhicule d'un État proliférant transitant par l'espace territorial des pays de la PSI[190]. Une telle disposition pourrait être complétée, le cas échéant, par des interdictions d'escale ou de transbordement pour les véhicules considérés.

Par ailleurs, l'élargissement du cadre d'action de la PSI à d'autres volets de la lutte contre les réseaux de prolifération mérite d'être étudié. Tout porte d'ailleurs à croire que l'Administration américaine pourrait vouloir étendre cette initiative à la lutte contre les flux financiers liés à la prolifération[191]. Reste que la PSI n'est, pour l'instant, qu'un outil permettant la coopération entre les militaires sur l'interdiction des mouvements de biens. Pour conserver la cohérence de l'initiative tout en l'étendant, il serait utile de mettre en place une instance de coordination et de décision de haut niveau rassemblant les acteurs concernés.

Au-delà de l'utilisation des forces armées pour des opérations d'interdiction, l'utilisation directe de la force contre les personnes animant les réseaux mérite d'être examinée. Sans aller jusqu'au changement de régime, la mise en place d'opérations clandestines contre les parties internes des réseaux pourrait constituer un moyen d'en réduire l'efficacité, voire dans certains cas de les neutraliser durablement. En référence à l'exemple irakien, la neutralisation des personnes coordonnant les travaux du MIC et des services secrets aurait vraisemblablement réduit la capacité du réseau à fonctionner efficacement. Bien que cela soulève des problèmes d'ordre juridique, il conviendrait d'approfondir les conditions – légales mais également techniques et politiques – dans lesquelles des actions contre des membres d'un réseau pourraient être entreprises.

L'action armée préventive contre les programmes étatiques eux-mêmes doit également être considérée. On ne peut que constater que l'opération *Iraqi Freedom*, outre la neutralisation définitive du réseau irakien, a permis de précipiter la décision de la Libye de renoncer à ses ambitions nucléaires. En dehors d'une utilisation massive de la force dans un objectif de renversement des régimes proliférants, qui semble dans l'immédiat peu crédible du fait de la situation des forces armées américaines[192], des actions ciblées moins exigeantes en termes logistiques peuvent permettre de peser sur les activités des réseaux et des programmes qu'ils servent.

[190] La fouille systématique de tout véhicule quittant l'espace territorial d'un État peut être envisagée par exemple dans le cadre d'une résolution *ad hoc* du Conseil de sécurité comme celle prise contre la Corée du Nord après l'essai du 9 octobre 2006.

[191] Entretiens de l'auteur novembre 2006.

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

## Conclusion

Les deux exemples qui ont été analysés en détail dans cette étude, le réseau de Abdul Qader Khan et l'organisation d'acquisition irakienne, illustrent les principes de fonctionnement et d'organisation qui semblent structurer la plupart des réseaux de prolifération existant.

Il en ressort en particulier l'importance de la coordination entre la gestion des flux – financiers comme physiques – et l'expertise technique, c'est-à-dire la connaissance des systèmes et des composants vendus comme achetés. Ainsi, pour bien fonctionner les réseaux doivent être capables de mouvoir discrètement des fonds, destinés à payer les diverses parties prenantes, de sélectionner les biens requis par les utilisateurs et de les acheminer jusqu'à eux. Pour y parvenir, ils s'appuient à la fois sur des agents qui leur appartiennent – qu'il s'agisse de personnes physiques, de sociétés ou encore d'établissements financiers – mais également sur une série d'intervenants – banques, fournisseurs ou sociétés de service – qui ignorent ou ne cherchent pas à savoir pour qui ils travaillent.

Il convient également de souligner que les réseaux ont su tirer le meilleur parti de l'essor du commerce mondial et de ses conséquences. Ils ont su exploiter à leur profit la dissémination des technologies pour se fournir auprès de sociétés implantées dans des pays ne possédant pas de systèmes de contrôle des exportations. De même, ils ont été capables de dissimuler leurs flux financiers et physiques en multipliant les intermédiaires et les sociétés écrans et en dématérialisant leur mouvement de fonds.

Pour autant, la « globalisation » constitue également une source potentielle de risque pour le fonctionnement des réseaux de prolifération. En effet, la dépendance grandissante des sociétés et des banques envers le marché mondial les rend plus sensibles à des sanctions qui les couperaient de celui-ci. Ainsi, les mesures prises par le département du Trésor américain pour interdire l'accès au marché américain à la *Banco Delta Asia* ont conduit cette dernière à geler les avoirs nord-coréens qu'elle gérait. Qui plus est, la publicité qui est faite autour de ces mesures est de nature à créer des effets d'entraînement sur un ensemble plus vaste de sociétés potentiellement concernées voire sur les États dans lesquels elles sont implantées. Ces derniers se trouvent également confrontés à des contraintes croissantes en termes de contrôle des exportations et des flux matériels transitant par leur territoire sous peine de se voir pénaliser en matière commerciale. S'en suit un début de renforcement des pratiques de contrôle, de la part de pays qui avaient servi aux réseaux de plates-formes logistiques comme Dubaï ou encore Singapour.

Quoiqu'il en soit, on ne peut aujourd'hui que constater la nécessité de mettre en place ou de renforcer les outils existants pour lutter contre les réseaux de prolifération. Pour structurer une telle démarche, la première étape devrait être l'élaboration d'une politique d'ensemble visant à coordonner les actions de renseignement, les outils de répression et les moyens d'interdiction. Chacun de ces piliers joue en effet un rôle particulier et unique afin de parvenir à la neutralisation pérenne des réseaux de prolifération :

- Cartographier la structure et l'organisation, détecter les opérations et suivre les flux.
- Neutraliser durablement des agents, des fournisseurs ou des intermédiaires clefs.

➥ Interrompre ponctuellement des flux matériels ou immatériels.

Il s'agit notamment d'assurer un équilibre entre les actions de long terme, qui doivent permettre de démanteler une organisation, et les opérations de court terme, qui peuvent avoir un sens d'un point de vue de sécurité mais sont de nature à compromettre les premières. Adaptées à chaque cas particulier, les stratégies de lutte contre les réseaux de prolifération devraient suivre trois axes principaux :

➥ Interrompre les flux financiers entre les banques appartenant au réseau et les établissements financiers extérieurs.

➥ Concentrer les mesures de répression sur les intermédiaires et les compagnies écrans.

➥ Neutraliser les activités logistiques – production et mouvement.

La lutte contre les réseaux de prolifération doit donc s'inscrire dans une logique interministérielle et internationale, mais elle doit aussi s'appuyer sur un renforcement de la coopération entre les administrations concernées et le monde industriel et financier. C'est dans ce dernier domaine qu'il existe aujourd'hui une marge de progression importante. En particulier, il est devenu essentiel de faire évoluer les outils de lutte contre les flux financiers illégaux pour traiter la problématique du financement des réseaux de prolifération. Un élargissement du mandat du Groupe d'action financière internationale (GAFI) à la question des trafics de prolifération permettrait en la matière de renforcer la coopération internationale, tant dans le domaine du renseignement que dans celui de la neutralisation des agents des réseaux. Des pistes pourraient également être explorées pour mieux adapter les systèmes de contrôle des exportations à la lutte contre les réseaux de prolifération. Dans la mesure où ils sont devenus des éléments clefs pour le fonctionnement des réseaux, les intermédiaires devraient faire l'objet de mesures ciblées. En particulier, la mise en place de lois cohérentes réglementant le courtage et le rendant illégal pour ce qui concerne les armes non conventionnelles s'impose.

Enfin, l'adoption par le Conseil de sécurité des Nations Unies de la résolution 1540, mais surtout de la 1718 qui cible les activités nord-coréennes, pose les bases d'une action internationale coordonnée contre les flux physique et financier de prolifération. Si la *Proliferation Security Initiative* offre à première vue un cadre séduisant pour coordonner l'action internationale, du fait de son degré d'avancement, son caractère essentiellement militaire la rend peu à même de remplir cette tâche. Qui plus est, on peut légitimement s'interroger sur la pérennité de cette instance qui dépend fortement de l'investissement de l'Administration américaine. Il conviendrait donc, avant d'étendre son domaine de compétence à la coordination des actions de répression, de réfléchir aux moyens d'en formaliser le cadre opérationnel.

# BIBLIOGRAPHIE


- « The Diffusion of Military Technologies and Ideas », Edited by Emily O. Goldman & Leslie C. Eliason, Standford 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 Standford, 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 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 Quaterly*, Spring 2005.
- John P. Caves Jr, « Globalization and WMD Proliferation Networks: The Policy Landscape », *Strategic Insights*, Vol. V, Issue 6, June 2006.