NOTE DE LA FRS

Pour une politique cohérente de lutte contre les réseaux de prolifération

Guillaume Schlumberger, Directeur
Bruno Gruselle, Chargé de recherche

(4 janvier 2007)

Les réseaux de prolifération fonctionnent comme des entreprises[1]. Ils doivent en effet être capables de coordonner une série de fonctions élémentaires : logistique, financière et technique.

Du fait de l'accroissement des échanges mondiaux, le seul renforcement des outils de contrôle des exportations existant ne saurait suffire à faire face au développement des flux de prolifération. Malgré leur médiatisation, les opérations d'interdiction[2] ne peuvent également avoir qu'un effet limité sur les réseaux , du fait de leur nature ponctuelle, si elles sont entreprises indépendamment d'une démarche ciblant les autres fonctions. Il paraît aussi peu réaliste de vouloir neutraliser un réseau de prolifération uniquement en gelant une partie de ses avoirs dans le cadre d'une démarche répressive[3].

La mise en place d'une politique d'ensemble visant à coordonner, au niveau national comme international, les actions de renseignement, les outils de répression et les moyens d'interdiction apparaît donc comme la seule solution viable pour lutter contre les réseaux de prolifération.

---

[1] B. Gruselle & G. Schlumberger, « Réseaux de prolifération : entre Sopranos et Supermarché », Notes de la FRS, juillet 2006.

[2] 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).

[3] 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, d'arrêter un intermédiaire, 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.

Il s'agit là d'une tâche complexe : elle nécessite en effet la structuration des responsabilités interministérielles et, surtout, elle passe par un équilibre entre les actions de long terme et le court terme. Elle repose enfin sur le renforcement des liens entre les administrations impliquées et les acteurs privés : sociétés de service, établissements financiers ou encore entreprises.

Le renseignement, outil central pour la lutte contre les réseaux

Afin de lutter efficacement contre les réseaux de prolifération, la première étape consiste à conduire un travail de cartographie (structure et modes opératoires des réseaux) et exige une capacité de renseignement dans les divers domaines dans lesquels les réseaux sont impliqués.

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. Par exemple, la surveillance d'un intermédiaire identifié du réseau Khan a pu permettre de repérer les entreprises fournisseuses, les banques intermédiaires et éventuellement d'autres agents appartenant au réseau[4]. Deux chausse-trappes semblent devoir être évitées dans cette démarche : 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[5]. *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.

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 contre une transaction particulière ou contre un acteur jugé suffisamment important pour que sa neutralisation affecte durablement les activités du réseau[6].

En termes d'organisation du renseignement national, les trois grands pays occidentaux – États-Unis, Royaume Uni et France – disposent d'outils relativement similaires : un service de sécurité intérieure et une ou plusieurs organisations dédiées au renseignement extérieur. L'ensemble permet à la fois de suivre les activités d'éventuels réseaux sur son territoire et leurs ramifications à l'extérieur.

---

[4] http://www.armscontrolwonk.com/1140/urs-tinner

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

[6] 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 le domaine financier, les États-Unis ont, en outre, créé une structure dont la particularité est d'intégrer les outils de renseignement et les moyens d'action contre les réseaux, y compris au niveau international[7]. Créé au sein du département du trésor en 2004, l'*Office of Terrorism and Financial Intelligence* (OTFI) dispose en effet de pouvoirs juridiques permettant au gouvernement américain de cibler les banques agissant au profit des réseaux[8] et 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[9].

Enfin, 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.

Pour améliorer l'efficacité de la fonction renseignement, il paraît nécessaire d'approfondir **le dialogue entre les services et les sociétés sensibles de petite taille** : ces dernières constituent en effet une cible particulièrement attractive pour les réseaux du fait de leur vulnérabilité économique. La première étape consisterait à dresser et maintenir à jour une liste exhaustive des sociétés potentiellement concernées. Il conviendrait ensuite de définir la nature des échanges entre les sociétés et les services de renseignement. Par exemple 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. De même, la cellule TRACFIN reçoit des déclarations de soupçons mais assure également, en principe, un retour vers le déclarant[10].

---

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

[8] Il s'agit de :

- 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. 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 une institution étrangère désignée comme étant préoccupante en matière de blanchiment (« *of primary money laundering concern* ») du système économique américain.

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

[10] Sous deux formes : informations sur le traitement d'une déclaration spécifique et actions d'information, de formation et de sensibilisation ciblées ou non.

Comment parvenir à la neutralisation des réseaux ?

Vers la mise en place des bases juridiques

Depuis l'adoption de la résolution 1540 du Conseil de sécurité des Nations Unies en avril 2004, les efforts de lutte contre les réseaux de prolifération peuvent s'appuyer sur un cadre formel qui fixe les mesures clefs que doivent prendre les membres de l'organisation en la matière :

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 3 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** liés aux 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 contrôle de l'industrie des services – transport, affrètement, banques – la résolution 1540 se contente de recommander la surveillance des activités liées aux exportations *stricto sensu*. Par ailleurs, en première lecture, elle se limite à criminaliser la prolifération des armes non-conventionnelles conduite par des acteurs non étatiques[11]. En conséquence, et même si le texte est à dessein ambigu concernant la prolifération des États, son extension à ce cas paraît politiquement improbable : certains pays poursuivent légalement des activités de développement d'armes nucléaires et *a fortiori* de missiles.

La résolution 1718 du 14 octobre 2006[12], votée suite à l'essai nord-coréen du 9 octobre 2006, **pourrait devenir une référence en matière de lutte contre les réseaux de prolifération** dans la mesure où elle complète les dispositions de la 1540. 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 toute cargaison entrante ou sortante 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 services qui soutiennent le fonctionnement des réseaux et éventuellement de

[11] Voir les articles 1 et 2. On notera que le champ d'application est interprété de façon différente selon les États.
[12] Votée sous chapitre VII.

renforcer le dialogue entre le secteur privé et les services et agences chargés de la lutte contre la prolifération.

De la même façon, la résolution 1737 du Conseil de sécurité imposant des sanctions ciblées à l'Iran[13] applique des mesures de même nature au programme nucléaire de Téhéran en visant les activités des établissements et intermédiaires agissant pour le réseau d'acquisition. En établissant un comité chargé de sa mise en œuvre, elle ouvre la possibilité de modifier cette liste qui prend en compte les activités financières du réseau.

L'élargissement du champ d'action contre les réseaux de prolifération

La globalisation économique rend nécessaire la coordination des politiques des États producteurs de technologies et des pays abritant des activités de service[14] susceptibles d'être exploitées par les organisations se livrant au commerce d'armes de destruction massive. Des progrès ont été indéniablement réalisés depuis 2003, grâce au lancement de la *Container Security Initiative* et de la *Proliferation Security Initiative*, en matière de coopération sur le contrôle des flux. En particulier, elles ont permis la mise en place dans certains États ayant servi de relais aux activités des réseaux de systèmes de contrôle des exportations ou des biens en transit.

Mais, l'élaboration et surtout l'utilisation par les États **de listes de biens et de technologies** pour lesquels l'exportation et le transit sont en général soumis à l'obtention d'autorisations préalables ne sont pas sans poser de réels problèmes. Les systèmes complets et leurs principaux composants sont en général relativement bien contrôlés puisque leur utilisation finale ne soulève que peu d'interrogations. *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[15]. Pour un pays possédant des ressources administratives limitées[16], le poids de la gestion des demandes d'exportation ou de transit – y compris les documents de transport[17] – 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 améliorations sont néanmoins envisageables :

- **La mise en place de clauses « attrape-tout ».** 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

[13] http://www.mideastweb.org/1737.htm
[14] Financement, transport/affrètement, transbordement, intermédiation.
[15] Il suffit pour s'en convaincre de regarder les listes de biens élaborées par l'arrangement de Wassenaar.
[16] 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.
[17] Manifestes de cargaison en particulier.

faire[18]. 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 l'instar du contrôle des flux financiers – à la responsabilisation des sociétés[19].

- **La possibilité d'élaborer des listes de destinataires finaux suspects devrait être envisagée et généralisée.** De tels documents, malgré les difficultés politiques qui peuvent entourer leur création, présentent 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 être envisagée au sein de groupes multinationaux[20] afin de mieux coordonner les efforts d'un ensemble de pays.
- **Le renforcement de la précision exigée pour les documents de transport** doit être envisagé pour éviter des déclarations floues et inexploitables.

Lutter contre le financement des réseaux

Même si son action est aujourd'hui concentrée sur le blanchiment d'argent et le financement du terrorisme, l'adoption de la résolution 1540 donne **une base pour étendre le domaine du groupe d'action financière international (GAFI[21]) à la lutte contre le financement de la prolifération**.

Les recommandations du GAFI portent essentiellement sur 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 et de geler leurs avoirs. 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.

Disposer d'outils juridiques pour encadrer le métier d'intermédiaire

La généralisation de dispositions visant à encadrer les activités des intermédiaires revêt un caractère d'urgence. En effet, ces derniers jouent un rôle important dans le fonctionnement des réseaux en

---

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

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

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

[21] Créé en 1989 par le G-7, le GAFI comprend aujourd'hui 33 pays membres, ce noyau 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.

servant de principaux relais pour les tentatives d'acquisition à l'étranger[22]. 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[23], peu de pays possèdent des instruments juridiques visant les courtiers[24]. Quelques pays européens, dont la France, ont toutefois mis en place de tels outils. De son côté, le Conseil de l'Union Européenne a adopté en 2003 une position commune sur le contrôle des intermédiaires en armement[25]. Il s'agit, dans les deux cas, de :

- Recenser les courtiers opérant 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 il s'engage.
- Etablir un système juridique punissant les activités d'intermédiation non autorisées.

Bâtir un édifice interministériel et international cohérent

Au fur et à mesure que de nouveaux outils, de natures différentes, seront ajoutés à la palette des moyens destinés à lutter contre les réseaux de prolifération, la question de la cohérence d'ensemble devrait inévitablement se poser. En effet, agir contre les réseaux de prolifération ne peut relever d'une logique d'opérations ponctuelles et indépendantes mais doit s'inscrire dans une démarche internationale coordonnée et ciblant l'ensemble des fonctions des réseaux.

Or, force est de constater qu'il n'existe ni organisation, ni forum, dont la tâche consisterait précisément à coordonner les actions d'interception, les éventuelles opérations financières et le renseignement. La PSI constitue un cadre attrayant pour la création d'une telle organisation, puisqu'elle coordonne d'ores et déjà les actions d'interception. Toutefois, son caractère opérationnel et informel ne la destine *a priori* pas à une telle fonction. Il serait donc plus utile d'envisager la création d'une organisation dont le rôle serait de gérer l'utilisation de l'ensemble des outils disponibles pour neutraliser tel ou tel réseau et qui rassemblerait les diverses administrations concernées : trésor, douanes, défense et services de renseignement. Il reste à savoir dans quelle mesure une telle initiative serait de nature à améliorer sensiblement le niveau et la qualité des échanges de renseignement essentiels à son fonctionnement.

---

[22] B. Gruselle et G. Schlumberger, « Réseaux de Prolifération : entre Sopranos et Supermarchés », Notes de la FRS, juillet 2006, p.3.

[23] 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.

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

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

Il faut finalement garder à l'esprit que, quelles que soient les mesures et actions prises pour améliorer la lutte contre les réseaux de prolifération, leur impact économique sur les activités légitimes devra être pris en compte. Il semble en particulier **essentiel de trouver un équilibre entre le besoin de sécurité et les impératifs liés au développement international des acteurs privés, au risque de rendre inopérant les mesures qui pourraient être prises**.

Les opinions exprimées ici n'engagent que la responsabilité de leurs auteurs.

Guillaume Schlumberger, Directeur
Bruno Gruselle, chargé de recherche
b.gruselle@frstrategie.org