note n°03/13

FONDATION pour la RECHERCHE STRATÉGIQUE

Bruno Gruselle
Maître de recherche à la Fondation pour la Recherche Stratégique
Elisande Nexon
Chargée de recherche à la Fondation pour la Recherche Stratégique

Les réseaux de prolifération à l'heure des sanctions ciblées

(janvier 2013)

Il y a de cela presque dix ans, l'existence d'organisations dont le but était de vendre et d'acheter des biens destinés à des programmes d'armes de destruction massive était mise à jour par les révélations sur le réseau du physicien pakistanais Abdul Qader Khan. Ces événements ont précipité l'adoption de décisions importantes visant à cibler le fonctionnement de ces réseaux au travers de réponses internationales et nationales coordonnées visant l'ensemble des fonctions opérationnelles liées à ce type d'activité : flux financier, transport, transfert de technologie, etc.

Ainsi, le Conseil de sécurité des Nations Unies adopte notamment en 2004 la résolution 1540 enjoignant aux pays membres de mettre en place les dispositifs de contrôle et de surveillance nécessaires pour éviter le transfert des armes les plus destructrices aux groupes terroristes. A bien des niveaux, les leçons apprises dans le cadre des travaux sur les réseaux de prolifération ont également guidé la communauté internationale lorsqu'elle a mis en place les résolutions visant à limiter l'accès de la Corée du Nord et de l'Iran aux technologies à caractère proliférant.

C'est en effet au travers des décisions du Conseil de sécurité que la détermination internationale à faire évoluer les outils de lutte contre la prolifération s'est illustrée depuis lors. Ce dernier a notamment établi – dans le cadre des résolutions 1929 (2010) pour l'Iran et 1874 (2009) pour la République Populaire Démocratique de Corée – deux panels d'experts dont le rôle est de rapporter des éléments tangibles sur le fonctionnement

et l'efficacité de ces embargos ciblés. Récemment ces deux panels ont publié leurs rapports annuels. Le panel 1874 conclut qu'il reste de nombreux obstacles au fonctionnement efficace des résolutions et mesures qui s'appliquent à la Corée du Nord, en particulier celles ciblant les opérations financières. Ainsi, il souligne sa préoccupation : « *about the greater use by the Democratic People's Republic of Korea of trade-based money-laundering techniques by means of front companies it established or agents it controls to fund illicit procurements and receive proceeds of sales of weapons and weapons of mass destruction-related transfers* »[1].

Cependant, malgré les efforts entrepris pour interdire les opérations d'acquisition de biens de prolifération, plusieurs pays maintiennent aujourd'hui des systèmes structurés dont la finalité est d'obtenir (illégalement) sur le marché international l'accès à des biens, des machines et à des technologies. Ceux-ci sont destinés à alimenter les programmes d'armes de destruction massive ou de missiles que ces pays ont entrepris, généralement en violation de leurs engagements internationaux ou d'embargos internationaux visant ces programmes.

L'existence de réseaux de prolifération ne fait aucun doute quand l'on considère les objectifs techniques ambitieux que se fixent certains pays proliférants comme la Corée du Nord. Pourtant il existe des différences de fond entre les réseaux existants, notamment en termes de structures et d'organisation. Ces différences tiennent en général aux conditions de développement du réseau plutôt qu'aux méthodes employées pour parvenir à ses fins. Ainsi, même si ces organisations se structurent autour de fonctions similaires (spécification des biens/technologies, achat, gestion du transport et du stockage), plusieurs éléments font que les schémas de décisions, les modes de fonctionnement et les méthodes diffèrent d'un réseau à un autre.

En tout état de cause, les **réseaux s'appuient sur le marché international existant de biens et de services pour fonctionner.** Comme l'a fait remarquer le groupe d'action financière internationale (GAFI) en 2008, ils doivent s'adosser au système financier international pour conduire leurs acquisitions dans la mesure où ils traitent essentiellement avec des fournisseurs et des acteurs qui n'agissent pas volontairement et en connaissance de cause à leur profit[2]. La part d'illégalité dans les activités de ces organisations est souvent limitée à leurs propres opérations et à certaines des méthodes qu'ils emploient pour dissimuler la destination et la finalité des acquisitions qu'ils envisagent. L'implication du groupe bancaire britannique *Standard Chartered* dans les opérations conduites par des banques iraniennes soumises aux sanctions de la communauté internationale du fait de leur implication dans les programmes nucléaires et de missiles de Téhéran montre les difficultés inhérentes à l'application universelle de mesures visant à interdire l'exploitation du système économique globalisé[3].

Quelques éléments de définition

Avant de s'intéresser plus précisément aux méthodes mises en place par les réseaux de prolifération pour contourner les mécanismes nationaux et internationaux de contrôle, il paraît utile de fournir au lecteur quelques définitions des termes utilisés afin de mieux cerner le domaine étudié. S'il existe une acceptation relativement universelle (et juridiquement solide) des activités de financement de la prolifération, ni la notion de réseau, ni le périmètre des activités de prolifération, ni même les réalités opérationnelles que cette notion recouvre ne sont parfaitement établis. La démarche visant à les définir plus précisément permet d'illustrer de façon schématique la situation relative des divers acteurs impliqués dans un système ayant pour finalité d'acquérir des biens ou des technologies à caractère proliférant (cf. figure infra) :

⇒ ***Opération d'acquisition*** : désigne l'ensemble des actes destinés à permettre l'achat, le paiement et le transport d'un ensemble de biens obtenu auprès d'un fournisseur unique donné, depuis la spécification du besoin jusqu'à la livraison à l'utilisateur final. Ainsi, l'acquisition de biens proliférant regroupe des actions à caractère technique et commercial, des actes de financements de la prolifération – notion définie précédemment – et enfin des opérations permettant le stockage et le transport des matériels.

⇒ ***Organisation d'acquisition*** : ce terme fait référence au groupe qui se charge de diriger les processus d'acquisition. Il se charge de traduire les besoins techniques exprimés par les utilisateurs en objectifs matériels à atteindre. Il est également chargé de trouver les fournisseurs, de définir les méthodes pour les approcher et les payer ainsi que les routes utilisées pour transporter les biens. A la lumière des cas connus, on peut imaginer plusieurs types de groupes opérant dans le domaine de l'acquisition (et éventuellement de la revente) de technologies : il peut s'agir d'organisations permanentes entretenues par des États clients et dont le rôle est de fournir ces derniers en fonction de leur besoin ou encore, à l'autre extrémité du spec-

tre, d'individus travaillant à leur compte et chargés par les États clients d'obtenir certaines technologies et d'assurer leur livraison sur leur territoire.

⇒ Une organisation d'acquisition repose pour fonctionner sur ***un réseau de personnes physiques et morales*** qui lui permet de conduire ses opérations ou les facilite. Le réseau de prolifération utilisé par une organisation d'acquisition est généralement indépendant de l'État auquel l'organisation appartient. Il peut s'agir d'intermédiaires opérant au profit de cette dernière dans un pays cible pour contacter ou négocier avec un fournisseur, une société de fret ou un établissement bancaire / financier utilisés pour participer à des opérations spécifiques. Les organisations d'acquisition font également appel à des sociétés écrans pour dissimuler leurs actions – y compris le transport de biens – ou à des établissements financiers (plus ou moins) complices pour assurer les transferts de fonds nécessaires. Dans certaines circonstances, elles s'appuient sur des entreprises de fret, qu'elles détiennent ou qui coopèrent volontairement avec elles. Elles sont indispensables pour permettre la livraison du matériel acheté à sa destination finale. Enfin, certaines entreprises externes peuvent volontairement, pour des raisons pécuniaires ou mercantiles, fournir ou soutenir (techniquement, logistiquement, administrativement, juridiquement) les organisations d'acquisition[4].

⇒ Le but de ces réseaux est d'obtenir **des biens destinés aux programmes d'armes**. Dans les faits, ce dernier terme couvre un spectre très large d'objets matériels ou de technologies/savoir-faire/compétences immatérielles. Ainsi, du côté tangible, il faut inclure : les équipements et systèmes complets, les composants, les pièces détachées, mais également : les machines-outils, les logiciels et outils informatiques ou encore les moyens d'essai et de calibrage. Dans le domaine immatériel, la notion de bien regroupe les technologies (méthodes de fabrication, éléments de développement y compris les documents liés), les compétences (techniques et scientifiques) et les savoir-faire (fabrication, production, essai) et les services. Le concept de transfert de biens recouvre donc toutes les activités logistiques de participation au transfert d'un bien matériel ou non vers le destinataire final.

Il paraît également utile de souligner **le rôle des personnes physiques et morales qui sont amenées de façon involontaire** à intervenir au profit d'organisations de prolifération. Outre certains fournisseurs, de nombreux opérateurs financiers ou logistiques peuvent participer à une ou plusieurs opérations menées par des organisations d'acquisition ou par les réseaux liés. Dans cette catégorie, on pourrait ranger *a priori* certains États servant de plaques-tournantes (pour des flux physiques ou financiers) ou offrant des pavillons de complaisance. Toutefois, il convient de souligner que la plupart d'entre eux, dans la mesure où ils ferment délibérément les yeux sur les opérations conduites par les réseaux de prolifération, participent en réalité volontairement au fonctionnement de ces derniers.

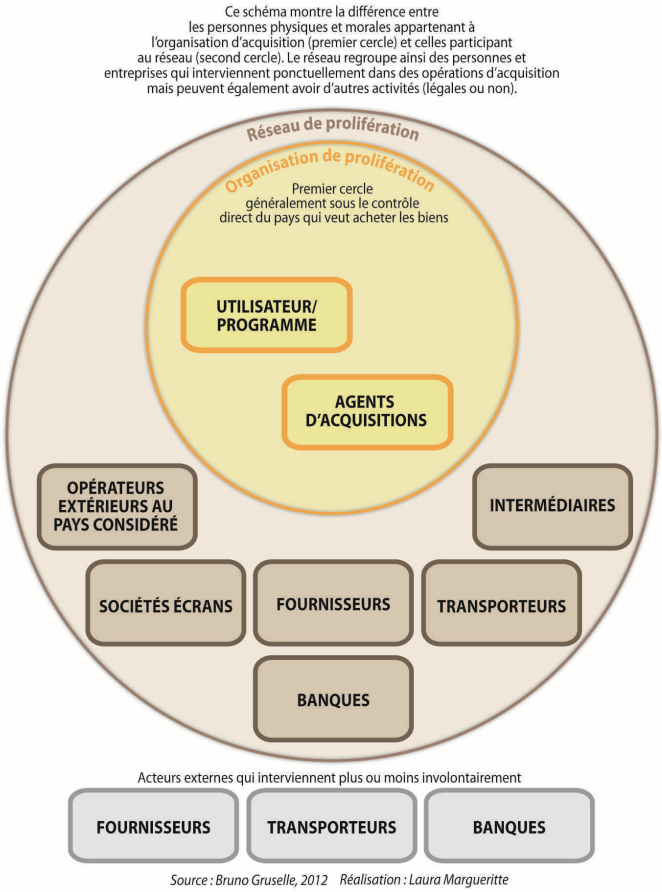

Figure 1 : Les différents acteurs des opérations d'acquisition de biens de prolifération (typologie schématique)

Les réseaux de prolifération ont évolué depuis dix ans sous l'influence combinée de l'extension des mesures de surveillance des flux et de l'universalisation des efforts de contrôle des exportations

Commençons d'abord par un constat : la structure des réseaux de prolifération ne s'est pas profondément modifiée depuis les révélations sur l'organisation d'Abdul Qader Khan en 2003. Les

opérations qui doivent être réalisées exigent toujours de pouvoir obtenir des biens auprès de fournisseurs plus ou moins complices en utilisant le système économique globalisé.

Ainsi, les réseaux continuent de se constituer autour de clients potentiels par l'agglomération d'acteurs qui agissent pour répondre à trois types de motivation : (1) ceux qui sont salariés plus ou moins directement par les proliférants, soit uniquement pour cette activité, soit pour elle parmi d'autres (agents, sociétés écrans, banques filialisées), (2) ceux qui cherchent à tirer profit du besoin des proliférants en agissant à la marge de la légalité (intermédiaires, entreprises complices) et enfin (3) ceux qui participent involontairement ou sciemment à une ou plusieurs opérations (ports de transit peu regardant, compagnies de fret, fournisseurs). Durant les dix dernières années, la dernière catégorie a été particulièrement ciblée par les efforts de lutte contre la prolifération et, dans les faits, de nombreux acteurs ont largement amélioré ou ont mis en place les mesures de contrôle interne permettant de réduire les risques de participer à des entreprises proliférantes.

Les réseaux continuent à transporter les biens destinés à leurs clients essentiellement par la voie maritime mais ils sont de plus en plus confrontés à des risques d'interdiction ou à la pression des contrôles douaniers ou policiers[5]. Ces risques se sont matérialisés y compris dans des ports de transit qui dans les années 1990 servaient de plaques-tournantes aux trafics à caractère proliférant (cas d'Abu Dhabi ou de Singapour). Les sociétés de fret de premier plan ont mis en place, sous la pression des États, des mécanismes permettant de mieux vérifier la nature des cargaisons et des biens transportés. Enfin, plusieurs États de pavillon de complaisance ont accepté des accords bilatéraux permettant aux pays occidentaux, notamment les États-Unis, de procéder à des fouilles en pleine mer sur des navires ou des cargaisons jugés suspects. On ne peut que souligner le rôle clef que la *Proliferation Security Initiative* (PSI) a joué pour restreindre les marges de manœuvre des réseaux en matière de transport maritime, tout en regrettant qu'elle continue à faire porter l'essentiel de son effort sur cette composante au détriment du transport aérien ou terrestre[6].

Pour répondre à ces mesures, les réseaux ont cherché à davantage dissimuler la nature et la destination des biens transportés (par le biais de fausses déclarations ou par le transport en pièces détachées), ont utilisé des sociétés de plus petite taille ou ont adapté en permanence leur flotte de transport aux mesures visant à en empêcher l'emploi pour des opérations de prolifération. Ainsi, l'*Islamic Republic of Iran Shipping Line* – entreprise ciblée par les sanctions du Conseil de sécurité qui possède l'une des flottes de commerce les plus importantes du Moyen-Orient – s'adapte en permanence pour échapper à la surveillance et utiliser ses navires pour des opérations légales ou illégales sans restriction.

Les réseaux et organisations de prolifération ont pu également continuer à utiliser le système financier international, et ce malgré les efforts ciblant les organismes bancaires participant directement aux efforts d'acquisition (gels d'avoirs, sanctions financières directes ou indirectes, etc.)[7]. Les sanctions financières ciblées et les mécanismes de surveillance – des instruments récents qui ont initialement été difficiles à généraliser au plan international – ont toutefois commencé à restreindre la capacité des organisations à utiliser les établissements bancaires employés jusqu'alors pour conduire leur transaction. Toutefois, les réseaux ont su s'adapter en passant par des banques relais moins regardantes ou moins bien équipées pour détecter des opérations frauduleuses, en utilisant des devises moins surveillées ou encore en achetant des établissements ou en créant des filiales. Il est vrai que les mécanismes mis en place pour détecter des opérations financières à caractère proliférant, conçus comme une évolution des moyens de lutte contre le blanchiment, sont relativement inadaptés à des opérations qui s'appuient sur des fonds légitimes pour conduire des actions illégales[8].

Comme le note le Groupe d'Action Financière International (GAFI) en 2010, les établissements bancaires ne disposent pas *a priori* d'instruments efficaces pour détecter à coup sûr si une transaction est proliférante ou pas[9]. En matière de lutte contre le blanchiment ou contre le terrorisme, c'est bien l'origine des fonds, en général déposés sous forme de liquidités, qui permet de repérer une opération frauduleuse. Pour l'acquisition d'un bien, les deux éléments tangibles sont l'identité de l'acquéreur et la nature du bien telle que décrite par les documents accompagnant la transaction. La généralisation du recours à des virements sans documentation technique rend la détection des tentatives d'acquisition de prolifération difficile sauf à savoir que l'une des parties est un acteur appartenant à un réseau.

Cette difficulté de fond, couplée au fait que les recommandations du GAFI en matière de lutte contre la prolifération sont encore insuffisamment appliquées par certains membres du groupe (pour des raisons matérielles, politiques ou culturelles), laisse à penser que les réseaux de prolifération continueront à s'appuyer sur le marché bancaire international pour conduire leurs opérations.

Enfin, les réseaux ont fortement modifié la structure de leur demande. Afin de tromper la surveillance des services chargés du contrôle, ils évitent les tentatives portant sur des composants dont le caractère proliférant est trop marqué (soit du fait de la nature du bien, soit du fait de ses performances ou caractéristiques techniques). S'agissant de passer sous « l'horizon radar », les réseaux vont plutôt cibler des biens extrêmement duaux voir des composants élémentaires en s'adressant à des fournisseurs de petite taille, moins susceptibles d'être sensibilisés aux problématiques de prolifération. L'autre solution est de s'adresser à des fournisseurs complices dans des pays qui eux-mêmes ne cherchent pas particulièrement à exercer un contrôle très strict[10].

L'efficience à moyen terme de ces adaptations de leurs méthodes, qui ont permis aux réseaux de poursuivre leurs activités dans la première phase de montée en puissance des mécanismes de contrôle, paraît difficile à établir. Elles sont effectivement confrontées à des mécanismes de contrôle et de surveillance qui restreignent de plus en plus les marges de manœuvre des opérateurs externes. Comme le souligne Alexander Montgomery en 2008, les réseaux ne peuvent plus fonctionner dès lors que les acteurs externes dont ils dépendent sont effectivement dissuadés de prendre part à des opérations suspectes ou illégales[11].

Pour répondre à ce double problème d'efficacité et de coût, plusieurs tendances d'évolution des mécanismes de contournement des moyens de surveillance, de contrôle et d'interdiction pourraient donc se dessiner à l'horizon 2020-2025 :

⇒ L'utilisation de modes de transport moins surveillés, en particulier la voie aérienne, pour les composants les plus sensibles : dans la mesure où les biens transportés sont plutôt peu encombrants, le choix du fret par avion se justifie autant sur un plan économique qu'en termes de difficultés à interdire réellement les expéditions. Cette tendance n'exclut pas le choix du transport par mer dans certaines situations particulières : biens de sensibilité limitée, utilisation de *hubs* moins surveillés (ports ouest-africains ou sud-américains plutôt que sud-asiatiques ou sud-africains) ou de compagnies de fret peu regardantes voir complices.

⇒ Le recours à ces transports alternatifs à la voie maritime correspond également à une tendance à la diminution de l'acquisition de biens matériels. Ce dernier pourrait être remplacé, d'une part, par l'acquisition de matières premières ou de composants élémentaires et, d'autre part, par l'achat de moyens de production modernes (machines-outils) qui ne soient ni particulièrement sensibles, ni spécifiques d'une activité de prolifération. Pour permettre à un tel système de fonctionner, les réseaux chercheront par-dessus tout à accéder à des compétences, des savoirs,

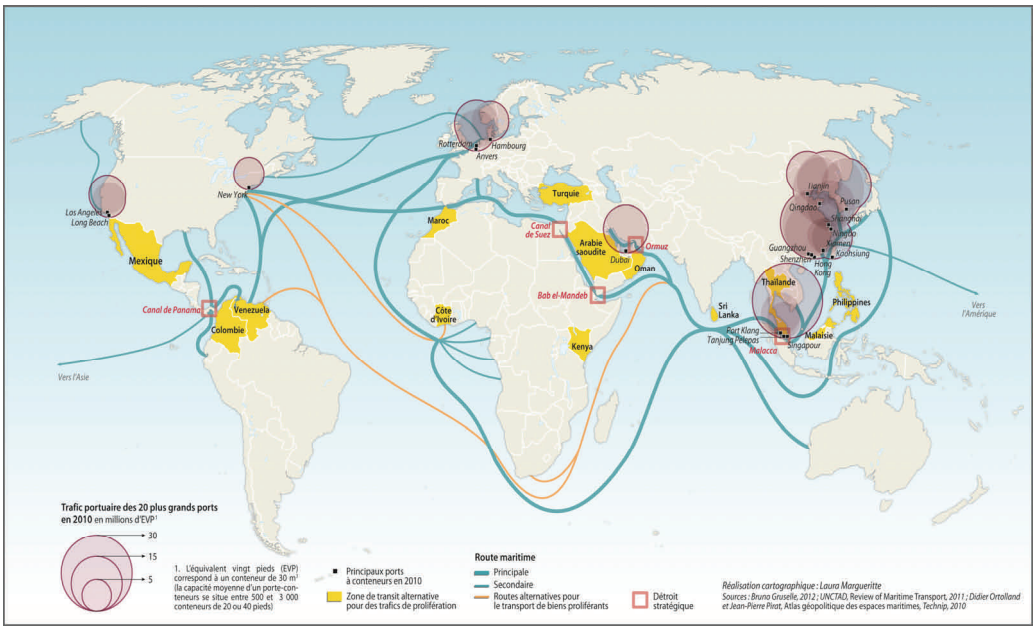

Figure 2 : Le contournement des routes principales de transit des biens est nécessaire pour les pays proliférants pour éviter le contrôle ou l'interception

Parmi les zones ou pays qui pourraient devenir attractifs pour le trafic mondial de biens de prolifération, il faut souligner l'émergence de l'Amérique du sud et, notamment, du Venezuela. Certains ports d'Afrique de l'Ouest pourraient également être concernés par ces efforts de contournement, comme par exemple la Côte d'Ivoire.

des savoir-faire et des technologies de préférence à des biens finis ou même des composants sensibles.

Il faut toutefois nuancer notre perception de l'efficacité d'une telle méthode pour ce qui est d'aboutir à des résultats concrets et applicables à des programmes d'armes (y compris de missiles). De fait, les exemples passés montrent incontestablement que la transmission du savoir et des compétences est une démarche difficile dont les résultats sont incertains, en particulier dans des environnements (et pour des programmes) qui se caractérisent par la compartimentalisation des tâches et la culture du secret[12]. Pour certains proliférants ayant de fortes dépendances techniques, cette solution paraît praticable à la condition de pouvoir accéder à un degré de soutien important (en termes de formation, d'assistance, etc.).

⇒ Les réseaux d'acquisition devraient continuer à s'appuyer sur le système financier international, mais leur dépendance envers les échanges classiques pourrait diminuer. Pour éviter les risques de gel d'avoirs ou de détection et diminuer les coûts associés au fonctionnement et à l'animation de nombreux établissements bancaires ou de sociétés écrans, d'autres méthodes de financement pourraient être adoptées. La montée en puissance des mesures visant à interdire aux réseaux et à leur client un accès libre aux principales devises pour leur transaction est également de nature à accélérer le désengagement des proliférants du système bancaire international. Pour compenser, les réseaux pourraient multiplier les accords de type troc tout en cherchant à élargir (y compris en termes géographiques) leur base de fournisseurs.

Ainsi, on devrait continuer à assister à des rapprochements entre les pays cherchant à accéder aux capacités non conventionnelles et les quelques États disposant de compétences mises en place depuis le milieu des années 1980 (Iran et Corée du Nord). Il est difficile de déterminer si les tendances actuelles en matière de généralisation/universalisation des règles de contrôle sont durables ou si elles aboutiront, à l'horizon considéré, à convaincre les quelques entreprises encore complices, en Chine notamment, à rompre les liens qui les rattachent encore à ces États. Toutefois, on peut imaginer que, sous la forte pression économique internationale (américaine, asiatique et européenne), la République Populaire impose peu à peu des mesures de contrôle et de vérification suffisamment dissuasives pour réduire les risques en la matière.

Les mécanismes de surveillance et de contrôle doivent continuellement être adaptés pour répondre à l'évolution des méthodes de contournement des réseaux de prolifération

Le succès des mécanismes internationaux mis en place pour ralentir les programmes iraniens et nord-coréens témoigne de l'efficacité d'une approche ciblant des domaines programmatiques spécifiques et dont les objectifs sont finalement relativement bien définis à l'avance.

La décennie qui s'est achevée aura donc permis l'émergence de cette nouvelle architecture de lutte contre la prolifération, au sein d'abord d'un petit groupe de pays, puis son extension progressive aux États alliés ou partenaires. Toutefois, les efforts d'adaptation des réseaux ont permis à ces derniers – moyennant des coûts économiques et financiers difficiles à estimer – de répondre au moins en partie à ces évolutions. En procédant en décembre 2012 au lancement réussi d'une fusée à trois étages *Unha*, qui pourrait servir de base à un missile de plus de 5 500 km de portée, la Corée du Nord a montré que ces dispositifs sont encore insuffisants mais surtout qu'ils ne s'adaptent pas assez vite pour faire face aux évolutions des réseaux[13]. Sur la base des éléments connus, les régimes de contrôle et d'interdiction devraient continuer à être renforcés pour encore restreindre les options des réseaux constitués.

On peut ainsi évoquer quelques pistes qui pourraient permettre d'améliorer le fonctionnement d'ensemble du système de lutte contre les trafics de prolifération.

Les efforts de contournement des mesures de surveillance et de contrôle des flux matériels par les réseaux et organisations de prolifération se concentrant sur l'utilisation de modes de transport et/ou de routes exotiques, il semble indispensable de développer les outils existants ou de les renforcer pour mieux prendre en compte la voie aérienne mais également la voie terrestre[14]. De fait, le recours possible à des « hubs secondaires » ou des routes alternatives nécessite d'étendre significativement l'empreinte géographique des différents mécanismes de contre prolifération.

Les zones les plus vulnérables, parce que situées dans des États en crise ou faillis, devraient faire l'objet d'une réflexion spécifique : il semble effectivement exclu de renforcer localement les mécanismes de contrôle et de vérification, mais il paraît possible de concentrer les moyens de recueil de renseignement pour mieux suivre les cargaisons passant par des ports situés dans ces

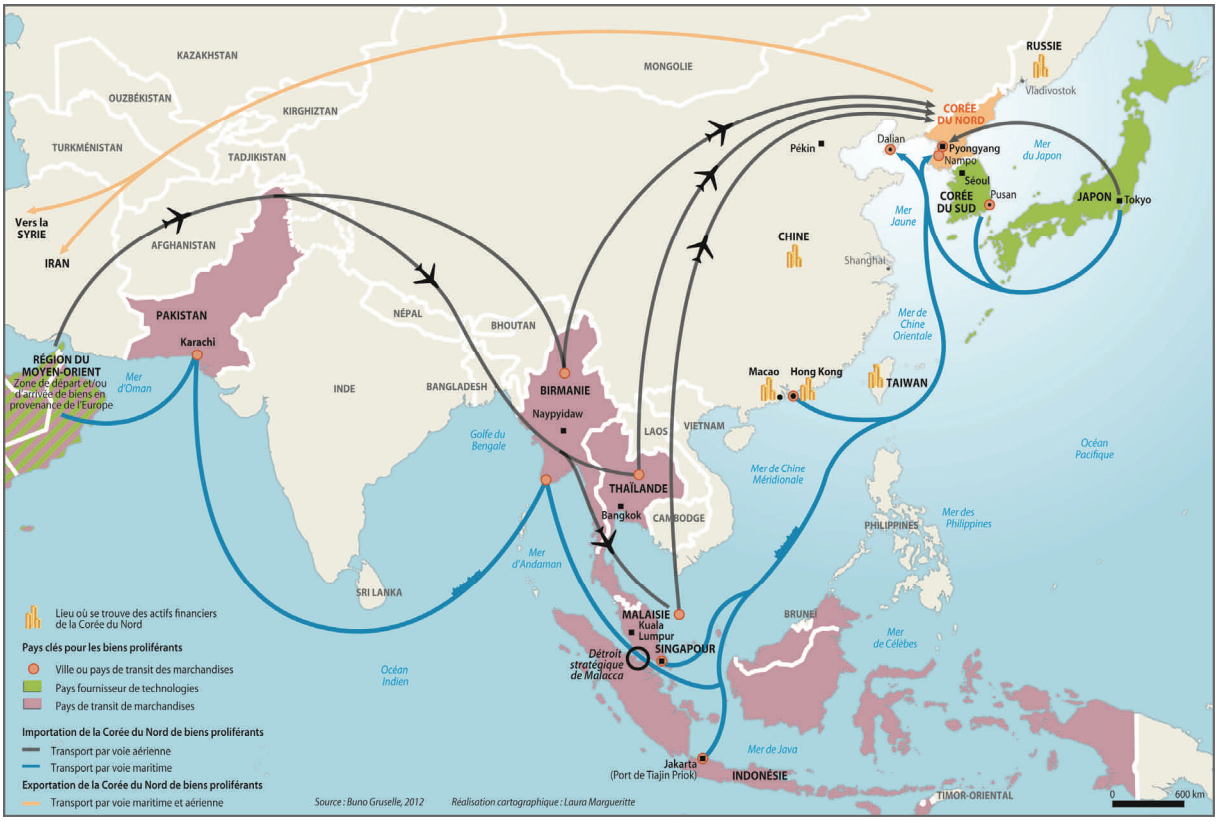

Figure 3 : Le réseau nord-coréen s'appuie d'abord sur des schémas d'acquisition locaux.

Il cible des fournisseurs en Asie, principalement au Japon, en Corée du Sud et en Chine, et fait transiter les biens par la Corée du Sud ou la Chine. Au niveau international, Pyongyang s'attache de façon croissante à transporter les biens par des voies évitant les points de passage obligés du transport maritime, qui sont les plus surveillés (notamment Singapour ou Dubaï). Il recourt de plus en plus au transport aérien et préfère à l'expédition de biens matériels, la fourniture d'une assistance et d'un soutien techniques.

pays.

L'extension de la *Proliferation Security Initiative* à la Chine, la Malaisie, l'Afrique du Sud, certains pays africains ou encore l'Inde représente également une certaine urgence[15]. C'est notamment le cas pour Pékin du fait (1) de la volonté chinoise de mettre en place ses propres routes maritimes afin d'éviter les zones se trouvant sous le contrôle direct ou indirect des États-Unis et (2) du poids relatif des hubs sous son contrôle (Shanghai et Hong Kong notamment) dans la gestion des flux maritimes (en particulier depuis et vers la Corée du Nord)[16]. La Malaisie, qui concurrence la place de Singapour comme premier port de commerce de la zone, ou encore la Thaïlande pourraient devenir des plaques-tournantes attractives pour les trafics des réseaux de prolifération depuis et vers l'Asie. De même, les ports d'Afrique (e.g. pour l'Ouest, la Côte d'Ivoire, et pour l'Est, le Kenya) pourraient voir leur intérêt s'accroître pour les réseaux de prolifération[17].

En matière de flux financiers, il semble utile de revoir avec les acteurs impliqués les conditions de fonctionnement des mécanismes de surveillance des opérations proliférantes. Si l'on exclut les sociétés, établissements et personnes visés explicitement par des sanctions, les banques se trouvent face à une difficulté majeure pour détecter des opérations à caractère proliférant. En effet, à la fois le caractère légal des fonds employés et l'absence d'informations documentaires sur l'objet des transactions rendent difficile voir impossible d'identifier une opération de ce type. Les banques ne peuvent finalement compter que sur les signalements qui peuvent être obtenus sur l'identité d'un des acteurs impliqués pour interdire une transaction suspecte. Cette situation donne un caractère encore plus pressant au besoin de disposer d'informations et de données utilisables (au sens du renseignement « *actionnables* » c'est-à-dire récentes et si possible à jour, précises et fiables) sur les personnes impliquées dans des réseaux de prolifération.

On ne peut pas non plus ignorer quelques signaux qui semblent montrer que certaines banques considérées comme honorables ont profité des sanctions internationales frappant les établissements iraniens clefs (Banques Melli et Saderat) pour réaliser des profits importants[18]. Toutefois, il faut supposer qu'il s'agit-là davantage de cas isolés plutôt que d'un effort de contour-

nement systématique des mécanismes de sanction existants.

Il est en revanche plus difficile de lutter contre les acquisitions qui impliquent des trocs, l'utilisation de systèmes de type Hawala ou des achats en cash « au dessus du comptoir » via des fonds transférés entre des individus habitant dans des pays différents[19]. Ce type d'opération pourrait toutefois se généraliser si les mécanismes interdisant le recours au système financier international se montrent plus efficaces à l'avenir. Pour répondre à de tels développements, la solution serait sans doute d'alourdir les mesures dissuasives pesant sur les acteurs nationaux impliqués. Aucune mesure d'ordre financier ne semble toutefois pouvoir être mise en place pour remédier au développement des coopérations dites sud-sud : seules les opérations d'interdiction physique des transferts paraissent être de nature à lutter contre une telle tendance.

Il est particulièrement important à ce titre de renforcer et de généraliser les mesures visant les transits (aériens et navals) et transbordements car, outre les possibilités d'interceptions en pleine mer – qui d'ailleurs sont plus difficilement faisables pour les expéditions par la voie aérienne –, il s'agit des seules occasions qui pourront être exploitées pour réellement fouiller un navire ou une cargaison, et le cas échéant confisquer cette dernière, et poursuivre les acteurs impliqués.

La problématique des transferts de technologies, de savoir-faire et de compétences devrait faire l'objet d'un traitement spécifique afin de répondre à la montée en puissance des offres d'assistance et de soutien. Ces dernières permettent dans les faits de contourner les mesures de contrôle physique. Les réseaux s'intéresseront sans doute davantage aux « ressources humaines » capables de soutenir scientifiquement ou techniquement les programmes – au travers par exemple de coopérations ou de *Joint Venture* – en s'appuyant sur des ressources matérielles très peu sensibles : calculateurs, logiciels du commerce, machines-outils banales… Pour parvenir à des résultats programmatiques tangibles, les réseaux devront toutefois déplacer de nombreuses personnes et même si une partie des transferts s'effectuera de façon immatérielle (documents sous format numérique, plans…).

Il apparaît particulièrement important que le secteur privé exerce à la fois un rôle de vigie et d'alerte, mais aussi qu'il contribue également à la régulation des flux immatériels – comme matériels ainsi que le soulignent les experts du panel 1874 dans leur rapport 2012[20] – notamment générés par les efforts internationaux que les entreprises peuvent être amenées à conduire dans le cadre des marchés exports. Il revient aux services des États, de s'assurer non seulement de la bonne prise en compte du risque dans les systèmes de surveillance internes des sociétés, mais également de développer les canaux de confiance leur permettant de communiquer sereinement avec elles sur des données et informations confidentielles ou sensibles.

Enfin, la tendance à la criminalisation des réseaux de prolifération, à la fois en termes de méthodes employées pour éviter les contrôles[21] mais également de recours à des acteurs criminels pour faciliter les efforts d'acquisition, mérite d'être prise en compte par un renforcement national et international des mesures légales. Il s'agit en définitive de faciliter la conduite des enquêtes et l'engagement de poursuites contre des personnes impliquées dans des opérations à caractère proliférant. Par ailleurs, il paraît important – en particulier si l'on détecte un rapprochement significatif entre organisations criminelles et réseaux de prolifération – de renforcer les efforts de coordination avec les services de police et les agences internationales (Europol, Eurojust et, éventuellement, Interpol) afin de favoriser le développement d'une communauté de sécurité étendue capable de s'attaquer à de tels phénomènes.◊

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

Bruno Gruselle
b.gruselle@frstrategie.org
Elisande Nexon
e.nexon@frstrategie.org

Notes

1. United Nations Security Council, *Report of the Panel of Experts established pursuant to resolution 1874*, 14 juin 2012.

2. Groupe d'Action Financière/Financial Action Task Force, « Proliferation Financing Report », 18 juin 2008.

3. « Le secteur bancaire au centre de plusieurs scandales retentissants », *La Tribune,* 7 août 2012 .

4. Groupe d'Action Financière/Financial Action Task Force, « Proliferation Financing Report », 18 juin 2008, pp. 35-36.

5. United Nations Security Council, « Report of the Panel of Experts established pursuant to resolution 1874 », 14 juin 2012, p. 37. Les experts soulignent que la Corée du Nord a progressivement plus de difficultés pour faire appel aux principales sociétés de transport maritime et pour accéder aux ports de transit indispensables pour le transport de biens depuis et vers son territoire.

6. Pour s'en convaincre, voir Mary Beth Nikitin, *Proliferation Security Initiative (PSI): Issues for Congress*, Congressional Research Service, 15 juin 2012.

7. Sonia Ben Ouagrham-Gormley, « Banking on Non Proliferation », *The Nonproliferation Review*, 2012, 19:2, pp. 241-265.

8. Ibid.

9. Groupe d'Action Financière/Financial Action Task Force, « Combating Proliferation Financing: A status report on Policy development and consultation », février 2010.

10. Cas de la Chine vis-à-vis de la Corée du Nord si l'on en croit l'épisode du véhicule de lancement exhibé en avril 2012.

11. Alexander Montgomery, « Proliferation Networks in Theory and Practice », in *Globalization and WMD Proliferation Terrorism, transnational networks, and international security*, Edited by James A. Russell and James J. Wirtz, Routledge 2008, p. 37.

12. Sonia Ben Ouagrham-Gormley, « Barriers to Bioweapons: Intangible Obstacles to Proliferation », *International Security,* Vol. 36, No. 4 (Spring 2012), pp. 80–114.

13. Voice of America, *S. Korea Says Debris Reveals North's ICBM Technology*, 23 décembre 2012.

14. United Nations, *Report of the Panel of Experts established pursuant to resolution 1929*, 12 juin 2012, p. 35.

15. Beth Nikitin, *Proliferation Security Initiative (PSI): Issues for Congress*, Congressional Research Service, 15 juin 2012.

16. Arms Control Wonk, *Hong Kong as Transshipment Point*, 3 mars 2011.

17. United Nations Conference on Trade And Development, *Review of Maritime Transport 2011*, New York 2011, pp. 86 -87.

18. « Le secteur bancaire au centre de plusieurs scandales retentissants », *La Tribune,* 7 août 2012 ; « The US says Iraqis are helping Iran to skirt sanctions », *The New York Times*, 18 août 2012.

19. United Nations, *Report of the Panel of Experts established pursuant to resolution 1929*, 12 juin 2012, p. 42.

20. United Nations Security Council, *Report of the Panel of Experts established pursuant to resolution 1874*, 14 juin 2012, p. 37.

21. Ainsi, l'utilisation de containers scellés avant leur introduction dans le flux international de biens permet d'éviter parfois leur contrôle par les autorités des ports de transit. En effet, une fois le container pris dans ce flux le risque d'inspection diminue fortement. United Nations Security Council, Report of the Panel of Experts established pursuant to resolution 1874, 14 juin 2012, p. 38.