SANCTIONS FINANCIERES CIBLEES

TYPOLOGIES DE FINANCEMENT DE LA PROLIFERATION

- MARS 2023 -

TABLE DES MATIERES

Sanctions financières ciblées 1
Typologies de financement de la prolifération 1
- Mars 2023 - 1
Table des matières 2
Introduction 3
Champ d'application du document de typologie 3
Coordonnées 3
Financement de la prolifération 4
Qu'est-ce que la prolifération ? 4
Qu'est-ce que le financement de la prolifération ? 4
Difficultés à détecter le financement de la prolifération 5
Financement de la prolifération – Études de cas 6
Utilisation (ou abus) du secteur bancaire 6
Recours à des personnes morales et accords (ou abus de ceux-ci) 7
Vente de biens 8
Cyberattaques 10
Signaux d'alarme liés au FP 11

INTRODUCTION

1. La Principauté de Monaco (Monaco), qui est un centre financier international, s'engage à protéger ses institutions financières (IF) et les entreprises et professions non financières désignées (EPNFD) contre les abus commis par des acteurs illicites impliqués dans le financement de la prolifération (FP) et d'autres initiatives de prolifération. Il est extrêmement important que l'ensemble de la population de personnes physiques et morales à Monaco fasse preuve de prudence et de vigilance pour que les individus ou les organisations soumis aux sanctions liées à la prolifération du Conseil de sécurité des Nations Unies (CSNU) ne soient en aucun cas soutenus.[1]

2. Le FP facilite la circulation et le développement de programmes relatifs aux biens sensibles à la prolifération et aux armes de destruction massive (ADM) et a le potentiel de contribuer à l'instabilité mondiale et à la perte de vies humaines. À ce titre, la prévention du FP est un élément important de la lutte contre la prolifération. Il est essentiel d'entraver les flux financiers dont disposent les auteurs de la prolifération et d'entraver et de compliquer l'achat de biens, de services et de technologies illicites nécessaires au développement d'ADM et de leurs moyens de livraison.

3. Le présent document de typologie relatif au FP présente des études de cas internationaux et des exemples sur la manière dont les personnes désignées (physiques et morales), groupes ou entités ont reçu un financement et un soutien malgré leur inscription sur les Résolutions du Conseil de sécurité des Nations Unies (RCSNU). L'objectif du présent document est de mettre en évidence les tendances et les méthodes utilisées par les personnes sanctionnées pour contourner les restrictions qui leur sont imposées par le CSNU. Une attention particulière est accordée aux RCSNU ciblant la République populaire démocratique de Corée (RCSNU 1718 (2006)) et la République islamique d'Iran (RCSNU 2231 (2015)).

4. Le présent document comprend également une liste de signaux d'alarme pouvant aider les IF et les EPNFD à détecter toute opération suspecte liée au FP.

Champ d'application du document de typologie

5. Le présent document de typologie a été publié par le Comité consultatif en matière de gel des fonds et des ressources économiques (le Comité consultatif) pour aider les entités déclarantes à mettre en œuvre des obligations liées aux sanctions financières ciblées (SFC). Les informations contenues dans le présent document ne constituent en aucun cas des conseils juridiques et doivent être lues conjointement à la législation nationale applicable, les normes internationales et les directives publiées par le Comité consultatif ou d'autres organismes compétents (par exemple, le SICCFIN et la DSP).

Coordonnées

6. Pour l'ensemble des demandes de renseignements, rapports et demandes concernant la mise en œuvre des contrôles de lutte contre le financement de la prolifération et les sanctions financières ciblées, veuillez envoyer un courriel au Comité consultatif en matière de gel des fonds et des ressources économiques.

E-mail : dbt.geldefonds@gouv.mc

Site Internet : https://geldefonds.gouv.mc

[1] Les Résolutions du CSNU liées au FP sont la RCSNU 1718 (2006) concernant la République populaire démocratique de Corée et la RCSNU 2231 (2015) concernant la République islamique d'Iran, ainsi que les résolutions qui leur succèdent.

FINANCEMENT DE LA PROLIFERATION

Qu'est-ce que la prolifération ?

7. La prolifération est définie par le Groupe d'action financière (GAFI) comme étant la fabrication illégale, le développement de l'acquisition, l'exportation, le transbordement, la négociation, le transport, le transfert, le stockage ou l'utilisation d'armes nucléaires, chimiques ou biologiques (ci-après dénommées collectivement les « ADM ») ainsi que leurs vecteurs et les matériaux connexes.

8. Dans sa RCSNU 1540 (2004), l'ONU définit la prolifération comme le transfert et l'exportation d'ADM, leurs vecteurs et les matériaux connexes. Cela pourrait inclure notamment la technologie, les biens, les logiciels, les services ou l'expertise. Elle définit en outre les « vecteurs » comme des missiles, des fusées et d'autres systèmes sans équipage capables de livrer des ADM spécialement conçues pour cette utilisation, et les « matériaux connexes » comme des matériaux, des équipements et des technologies couverts par les traités et accords multilatéraux pertinents, ou figurant sur les listes nationales de contrôle, qui pourraient être utilisés pour la conception, le développement, la production ou l'utilisation d'ADM et de leurs vecteurs.

Qu'est-ce que le financement de la prolifération ?

9. Suivant la définition ci-dessus, le « financement de la prolifération » (FP) est défini par le GAFI comme la *fourniture de fonds ou la prestation de services financiers* utilisés pour la fabrication, l'acquisition, la possession, le développement, l'exportation, le transbordement, la négociation, le transport, le transfert, le stockage ou l'utilisation d'ADM et de leurs vecteurs et des matériaux connexes (y compris les technologies et les biens à double usage utilisés à des fins non légitimes), en violation des lois nationales ou, le cas échéant, des obligations internationales.

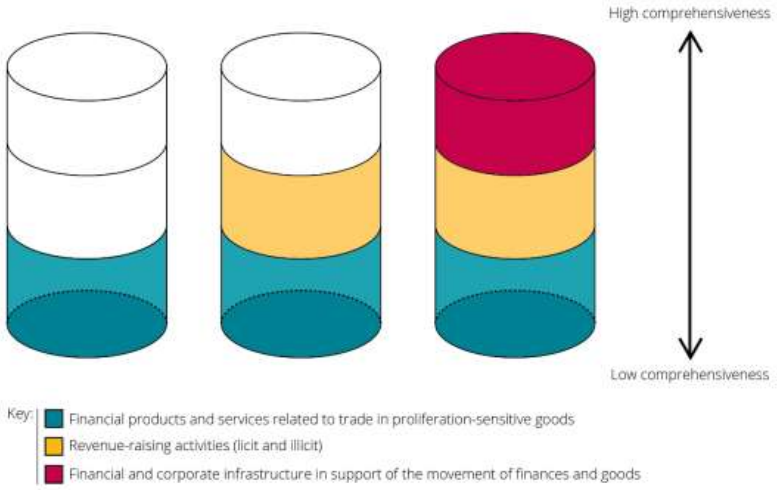
10. En d'autres termes, le FP vise à fournir des services financiers aux programmes liés au transfert et à l'exportation d'ADM, de leurs vecteurs et des matériaux connexes. Il s'agit également du financement du commerce de biens sensibles nécessaires à l'appui ou au maintien desdits programmes, même si ces biens ne sont pas liés à des ADM (biens à double usage), par exemple : pétrole, charbon, acier ou équipement de communication militaire (voir le tableau 1 ci-dessous pour plus d'exemples). En outre, le FP inclut le soutien financier aux personnes ou entités impliquées dans la prolifération, même si elles exercent d'autres activités qui ne sont pas liées à de tels programmes (par exemple diplomates, compagnies maritimes, secteur de la pêche, commerce de matières premières).

Tableau 1. Exemples de biens généraux à double usage

Armes nucléaires	Armes chimiques	Armes biologiques	Missile et livraison
Centrifuges	Épurateurs	Fermenteurs	Alliages d'aluminium
Caméras haute vitesse	Réacteurs	Séchoirs-atomiseurs	Oxydants
Composites	Refroidisseurs	Réservoirs	Machines-outils
Acier maraging	Ascenseurs	Broyeurs	Presses isostatiques
Pompes à vide	Échangeurs thermiques	Souches bactériennes	Composites
Jauges de pression	Navires de mélange	Filtres	Gyroscopes

11. Le FP étant un mélange 1) de services de paiement et financiers en soutien direct à l'approvisionnement en biens et au développement d'ADM, 2) de la levée de fonds et d'activités génératrices de revenus pour financer les efforts de prolifération, et 3) de réseaux et services financiers et d'entreprise qui soutiennent ces activités, le Royal United Services Institute[2] suggère de considérer le FP comme couvrant trois catégories d'activités qui devraient être étudiées dans le cadre des efforts de lutte contre la prolifération (LCP).

[2] « Guide to Conducting a National Proliferation Financing Risk Assessment » (« Guide d'évaluation nationale du risque financier de prolifération »), Royal United Services Institute, 2019



ANGLAIS	FRANCAIS
High comprehensiveness	Forte exhaustivité
Low comprehensiveness	Faible exhaustivité
Key	Clé
Financial products and services related to trade in proliferation-sensitive goods	Produits et services financiers liés au commerce de biens sensibles à la prolifération
Revenue-raising activities (licit and illicit)	Activités de collecte de recettes (licite et illicite)
Financial and corporate infrastructure in support of the movement of finances and goods	Infrastructure financière et d'entreprise favorable à la circulation d'argent et de biens

12. Les personnes désignées en vertu des RCSNU liées au FP sont susceptibles d'avoir recours à des réseaux complexes d'entreprises de façade et à des techniques de détournement qui miment les typologies de blanchiment de capitaux pour contourner les mesures de sanctions en matière de LCP et accéder au système financier mondial. Néanmoins, il existe des différences distinctes entre blanchiment de capitaux et violation des sanctions, le premier étant un processus circulaire déployé par des délinquants pour dissimuler l'origine illicite des produits de la criminalité tandis que la seconde concerne les personnes auxquelles des fonds sont mis à disposition (des personnes désignées) ou les fins pour lesquelles ils sont utilisés (prolifération).

13. En raison de leurs différences, les IF et les EPNFD devraient considérer le FP comme un type distinct de criminalité financière qui exige également un type différent de conformité aux sanctions. La section suivante permettra de mettre en lumière les cas réels de FP survenus dans différents secteurs, dans le but de sensibiliser davantage à ces sanctions et à l'importance de leur mise en œuvre.

Difficultés à détecter le financement de la prolifération

14. Il existe un certain nombre de difficultés liées à l'identification du financement de la prolifération :

- Une tendance croissante dans l'achat et la vente de composants élémentaires, par opposition à l'ensemble des systèmes manufacturés. Les composants élémentaires individuels peuvent également avoir des utilisations légitimes (biens à double usage), rendant leur identification à des fins illégitimes encore plus problématique.
- Les biens à double usage sont difficiles à identifier, nécessitent des connaissances spécialisées et peuvent être décrits en des termes communs pouvant être employés dans de multiples contextes, tels que les « pompes ».
- Les réseaux par lesquels des biens sensibles à la prolifération peuvent être obtenus ont tendance à être complexes. Cela, combiné à l'utilisation de fausses documentations, permet la prolifération des biens sensibles, des entités concernées, des transactions financières associées, et de l'utilisateur final ultime afin d'éviter la détection. Il est fréquent que des sociétés écran, agents et autres faux utilisateurs finaux soient utilisés pour couvrir l'utilisateur final réel.

- Le risque de financement de la prolifération est plus susceptible de se présenter dans les cas où la source des fonds est légale et que l'utilisateur final d'un type de biens en cause est caché, ce qui rend difficile l'identification de ces activités.

15. En définitive, en tant qu'IF ou EPNFD, il est essentiel de bien comprendre le risque de FP auquel vous êtes exposé(e) pour être en mesure de décider des mesures à prendre pour les atténuer. Les indicateurs relatifs au commerce énumérés ci-dessus peuvent contribuer à l'identification et à la classification des éventuelles menaces et vulnérabilités. Chaque IF ou EPNFD doit avoir sa propre politique en matière d'évaluation des risques. En outre, le FP doit être inclus comme un risque de criminalité financière spécifique lors de la formation ou de la conduite d'exercices visant à sensibiliser le personnel.

16. Comme indiqué ci-dessus, l'identification du FP est difficile parce que la plupart des transactions se déroulent dans le cadre normal des transactions commerciales, et peuvent être masquées par toutes les transactions légitimes. Selon le modèle commercial, l'on pourrait intégrer les indicateurs commerciaux dans les procédures de connaissance du client (KYC), les procédures de filtrage des transactions, les systèmes de surveillance des transactions et les enquêtes sur les activités suspectes, les procédures de déclaration réglementaire et les procédures de diligence raisonnable liées aux opérations de financement du commerce.

FINANCEMENT DE LA PROLIFERATION – ÉTUDES DE CAS

17. La section suivante permettra de mettre en lumière les cas réels de FP survenus dans différents secteurs, dans le but de sensibiliser davantage à ces sanctions et à l'importance de leur mise en œuvre.

Utilisation (ou abus) du secteur bancaire

Étude de cas 1 : Accès à un compte bancaire commercial légitime[3]

18. En juillet 2013, les autorités du canal de Panama ont détenu un navire nord-coréen, le Chong Chon Gang (CCG), alors qu'il transitait de Cuba vers la Corée du Nord. Les autorités du canal ont trouvé une cargaison d'armes et de matériels connexes dissimulés sous d'autres marchandises. Le CCG était exploité et géré par Ocean Maritime Management Company Ltd (OMM), l'une des plus grandes compagnies maritimes nord-coréennes. Les coûts liés au voyage du CCG ont été payés par Chinpo Shipping Company (Private) Limited, basée à Singapour.

19. L'ambassade de Corée du Nord à Singapour a utilisé l'adresse professionnelle comme adresse postale. Chinpo a accueilli le personnel d'OMM dans ses bureaux et a utilisé son compte bancaire pour gérer les fonds pour le compte d'OMM. Les sommes dues à OMM (par exemple, les frais de transport) ont été versées sur ledit compte. Les fonds ont été versés à partir du compte à la demande d'OMM, par exemple aux propriétaires de navires nord-coréens (qui n'ont pas été en mesure d'établir leurs propres comptes bancaires en raison de sanctions), ou en leur nom pour des fournitures, des frais portuaires ou d'autres débours, ou d'un armateur nord-coréen à un autre. Sur trois ans, 605 transferts de fonds ont eu lieu, soit plus de 40 millions USD, tous liés aux navires nord-coréens. Chinpo exerçait effectivement en tant que prestataire de services de transferts de fonds, bien qu'elle n'ait reçu des autorités singapouriennes aucune autorisation à ce titre. Une fois par an, un diplomate nord-coréen ayant accès au compte Chinpo retirait jusqu'à 500 000 USD en billets de banque à transférer hors du pays. Chinpo a tenté de cacher son implication auprès des sociétés nord-coréennes en retirant les noms des navires nord-coréens et d'autres détails d'identification des formulaires de transfert de fonds et de correspondance par e-mail, et les paiements du compte de Chinpo avaient lieu en l'absence de factures ou d'autres détails.

[3] « Countering Proliferation Finance : An Introductory Guide for Financial Institutions » (« Lutte contre le financement de la prolifération : Guide d'introduction à l'attention des institutions financières »), Royal United Services Institute, 2017

Étude de cas 2 : Maintien des bureaux de représentation et des agents à l'étranger

20. En février 2017, le Groupe d'experts des Nations Unies a obtenu des informations montrant que deux banques sanctionnées, Daedong Credit Bank (DCB) et Korea Daesong Bank (KDB), étaient toutes deux présentes sur le territoire chinois, par l'intermédiaire de bureaux de représentation à Dalian, Dandong et Shenyang. Un administrateur de ces bureaux a simultanément été administrateur d'une société désignée, DCB Finance Ltd., immatriculée aux Îles Vierges britanniques. DCB Finance partageait plusieurs agents avec DCB, et lorsque les comptes correspondants de DCB ont été clôturés en 2005, DCB Finance a été fondée pour effectuer des virements électroniques et des opérations commerciales pour son compte.

21. Le représentant à Dalian de DCB et de DCB Finance a effectué des transactions en dollars américains, certaines transactions uniques dépassant occasionnellement la barre de 1 million USD. Il a également facilité les paiements et les prêts entre les sociétés liées à DCB et a échangé de grandes quantités de liquidités transférées de la Corée du Nord à la Chine en billets en dollars américains en grosses coupures. En outre, le représentant a également procédé à des échanges de devises entre le dollar américain et l'euro, transférant des soldes entre DCB et son actionnaire (principalement la Korea Daesong Bank). Lorsque DCB a établi des bureaux de représentation à Shenyang à la fin de 2012, et à Dandong en 2014, les trois bureaux ont coopéré à la gestion des activités de change, de transferts, d'échanges de grandes quantités de liquidités et de prêts.

Étude de cas 3 : Achat de biens à double usage par le biais de transactions financières[4]

22. Un courtier a été impliqué ; il était de nationalités iranienne et européenne, et disposait d'une résidence dans un État membre de l'UE et d'un compte bancaire dans cet État membre de l'UE. Ce courtier était immatriculé dans les îles Vierges britanniques (IVB) et menait ses activités par l'intermédiaire d'une société écran. Les autorités pourraient associer cette dernière à au moins une société iranienne. Cette société écran détenait un compte auprès d'une banque nationale à Dubaï et avait également un compte bancaire dans un État des Balkans, membre de l'UE.

23. Une banque iranienne était à l'origine des fonds. Le paiement a été effectué par une succursale de cette banque à Dubaï sous la forme d'un virement électronique sur le compte de la société écran à Dubaï. Des fonds ont été transférés de ce compte à des fournisseurs au Luxembourg ainsi qu'à des particuliers dans plusieurs États membres de l'UE.

24. Les enquêteurs n'ont trouvé aucune preuve que des biens à double usage étaient impliqués dans l'une ou l'autre des transactions financières, mais ils soupçonnaient que le mécanisme pouvait servir à financer la prolifération.

25. Les clients iraniens détenant des comptes bancaires au Luxembourg ont également viré de l'argent sur le compte européen du courtier basé aux IVB. Les canaux ont été utilisés à plusieurs reprises dans certains cas (lorsque les fournisseurs européens étaient impliqués) et parfois seulement une fois (lorsque des particuliers étaient impliqués).

Recours à des personnes morales et accords (ou abus de ceux-ci)

Étude de cas 1 : Achat de biens par l'intermédiaire de tiers

26. La cellule de renseignements financiers (CRF) des Émirats arabes unis (EAU) a reçu une déclaration de soupçon de la part d'une banque dans laquelle la Personne X détenait deux sociétés, dont l'une était soupçonnée d'acheter des équipements d'aéronefs à des sociétés établies dans un autre pays. Ces équipements ont été expédiés à une société basée aux EAU qui travaillait pour le compte d'une entité inscrite sur la liste de l'OFAC qui pourrait soutenir le programme nucléaire iranien.

27. Les autorités des Émirats arabes unis ont confirmé que la Personne X et ses sociétés entretenaient une relation d'affaires avec une entité listée et que la société était utilisée pour couvrir le bénéficiaire final des équipements achetés afin d'éviter les sanctions. Suite à cette constatation, une ordonnance de gel a été rendue sur les comptes bancaires personnel et professionnel de la Personne X.

28. Le Parquet Général des Émirats arabes unis a confirmé qu'il avait des motifs raisonnables de soupçonner une violation des sanctions d'après les rapports d'enquête, et a ordonné une arrestation de la Personne X et le gel des fonds et d'autres avoirs d'une valeur de 4 800 000 AED (environ 1 200 000 EUR).

[4] « Study of Typologies of Financing of WMD Proliferation: Final Report » (« Étude des Typologies du Financement de la prolifération des ADM : rapport final »), Jonathan Brewer, 2017

Étude de cas 2 : Création de coentreprises pour générer des revenus

29. Une enquête sur Korea General Corporation for External Construction (GENCO/KOGEN) par le Groupe d'experts des Nations Unies a révélé que l'entreprise disposait d'un vaste réseau et se prévalait d'une importante présence dans plusieurs pays du Moyen-Orient, d'Afrique et d'Eurasie, où elle faisait appel à des travailleurs, des entités coopératives et des coentreprises de la Corée du Nord pour gagner des revenus importants. Un pays a affirmé que GENCO/KOGEN « a œuvré à la mise à disposition d'ouvriers nord-coréens au Moyen-Orient dans le but de rapporter des devises fortes pour la Corée du Nord ». Des éléments de preuve suggéraient qu'une coentreprise entre GENCO/KOGEN et une société des EAU soutenait les activités de l'entreprise.

30. Les documents d'enregistrement des sociétés indiquaient que GENCO/KOGEN était l'un des propriétaires d'une entité coopérative de construction/coentreprise en Russie, dont la propriété majoritaire appartient à un ressortissant russe. Cette personne morale détenait un compte auprès d'une banque russe. En outre, il a été constaté que la société russe avait les mêmes adresses, coordonnées et actionnaires que trois autres sociétés, toutes impliquées dans des activités liées à la construction. En outre, les documents du registre des sociétés montrent que GENCO/KOGEN exploitait deux bureaux de représentation officiels en Russie qui employaient officiellement 17 ressortissants nord-coréens.

31. Outre sa présence en Russie, GENCO/KOGEN était présente au Nigeria, en Côte d'Ivoire et en Guinée équatoriale. Au Nigéria, elle a été immatriculée en tant que « Korea General Company for External Construction GENCO (Nigéria) » et en Côte d'Ivoire en tant que « Korea General Construction SL (KOGEN GE SL) ». Par ailleurs, le Bureau Interafricain des Ressources Animales de l'Union Africaine a répertorié KOGEN GE S.L. sur son site Internet, déclarant que cette société était un partenaire dans le cadre de la mise en œuvre d'un projet financé par la Guinée équatoriale. GENCO/KOGEN a été déclarée séparément en tant qu'entrepreneur pour le Stade Municipal de Rebola, dont les bénéfices étaient estimés à environ 30 500 000 USD.

Étude de cas 3 : Émission d'assurances non autorisées

32. DGS Marine était une société commerciale offshore immatriculée au Liechtenstein, située dans un bureau de fiducie à Vaduz jusqu'à mi-2012. Des rapports de médias ont révélé que le directeur de DGS, David Skinner, avait émis des certificats d'assurance pour les pétroliers appartenant à l'Iran transportant du pétrole en provenance de Syrie prétendument en violation des sanctions de l'Union européenne. À la suite des rapports, l'Autorité financière du Liechtenstein a émis un avertissement indiquant que DGS Marine n'était pas autorisée à souscrire des assurances au Liechtenstein. Après l'avertissement, l'administrateur a fait immatriculer DGS Marine en tant que société commerciale basée dans les Îles Vierges britanniques (IVB) un mois plus tard, même si le Groupe d'experts des Nations Unies a également été en mesure de confirmer peu de temps après que DGS Marine n'était pas titulaire d'un permis ni autorisée à souscrire des assurances dans les IVB.

33. Avant 2012, il a été constaté que le rapport annuel de la société contenait de fausses informations concernant l'identité du commissaire aux comptes indépendant de DGS, remettant en cause la certification des déclarations financières annuelles de DGS Marine. DGS Marine n'a pas répondu aux demandes du Groupe d'experts des Nations Unies. À la suite de l'enquête, les médias ont indiqué que DGS Marine était une escroquerie d'assurance sophistiquée qui, tout en maintenant des bureaux au Royaume-Uni, à Chypre, au Danemark, au Vietnam, en Inde, en Chine et aux Émirats arabes unis, ne possédait pas les millions de livres en valeurs mobilières déclarés dans ses rapports annuels.

Vente de biens

Étude de cas 1 : Transbordements entre navires

34. Les transbordements entre navires sont devenus un moyen fréquent de violation de sanctions, dont la régularité et la valeur ont battu des records depuis 2018. L'enquête menée par le Groupe d'experts des Nations Unies sur les transferts de pétrole a mis en évidence un exemple très sophistiqué d'usurpation d'identité des navires liés à la Corée du Nord, en soulignant les nouvelles techniques de violation de sanctions qui ont rendu vains les efforts de diligence raisonnable du premier négociant en matières premières de la région, ainsi que les banques américaines et singapouriennes qui ont facilité les paiements de carburant et un assureur britannique de premier plan qui apportait une protection et une indemnisation à l'un des navires impliqués. Cette même affaire souligne l'extrême faiblesse du système d'établissement de rapports, du contrôle et de la surveillance des navires exercés par les États de pavillon de complaisance relevant du territoire sur lequel ils naviguent apparemment, ainsi que l'absence de mise en œuvre des décisions de gel.

35. En 2018, quatre navires ont été jugés en violation de la RCSNU 2375 (2017), leurs activités étant principalement basées dans la province de Taïwan, en Chine, tandis que leurs sociétés sont immatriculées dans plusieurs juridictions, dont les IVB, Hong Kong, les Îles Marshall, Samoa et Seychelles, et des navires battant pavillon de la République dominicaine, de Hong Kong, du Panama et de la Sierra Leone.

36. Deux des quatre pétroliers (Lighthouse Winmore, sous le pavillon de Hong Kong, et le Billions No. 18, sous le pavillon du Panama) ont transféré le diesel maritime à des pétroliers battant pavillon de la Corée du Nord. Depuis la Corée du Sud, les pétroliers ont désactivé leur système d'identification automatique quelques jours avant et après les transferts. D'autres soupçons ont été soulevés lorsque les deux pétroliers sont retournés au port de départ, au lieu de naviguer vers le port d'arrivée prévu qui se trouvait à Taïwan. La République de Corée a retenu le Lighthouse Winmore pour le soumettre à enquête le 24 novembre 2017.

37. Ces enquêtes sur le Lighthouse Winmore ont mis en évidence que le pétrolier a été affrété peu avant le transbordement entre navires par Oceanic Enterprise Ltd, une société des Îles Marshall, par l'intermédiaire d'un courtier basé à Singapour. L'unique administrateur et actionnaire de la société était Shih-Hsien Chen, ressortissant taïwanais.

38. L'on a constaté que deux des pétroliers de M. Chen, le Lighthouse Winmore et le Golden Rich, faisaient appel au même titulaire de document de conformité et gestionnaire international de la gestion de la sécurité. Les connaissements pour les produits pétroliers embarqués par le Lighthouse Winmore et le Billions No. 18 avant le transfert indiquent la multinationale Trafigura Pte. Ltd. en tant qu'expéditeur, Global Commodities Consultants Ltd. en tant que destinataire et le port de Taichung comme destination. Global Commodities est immatriculée à Hong Kong, mais son siège social correspond à celui de la société singapourienne, Global SGP Pte Ltd. Les deux sociétés partagent le même administrateur et actionnaire unique.

39. Oceanic Enterprise a payé un acompte à Global SGP Pte Ltd. pour les deux expéditions livrées aux navires (d'un montant total d'environ 13 000 000 USD) par le biais de virements bancaires au fournisseur, avec lequel elle avait conclu un contrat. En plus de ces deux transferts par le Billions No. 18 et le Lighthouse Winmore, Oceanic avait prévu neuf autres expéditions d'une valeur estimée à environ 65 000 000 USD.

Étude de cas 2 : Vente de biens à double usage

40. En collaboration avec les EAU, le Bureau de contrôle des avoirs étrangers (OFAC) du Département des Finances des États-Unis a désigné 11 entités et personnes impliquées dans les achats pour le compte du programme de missiles balistiques de l'Iran. L'OFAC a sanctionné Mabrooka Trading Co LLC (Mabrooka Trading) – basée aux Émirats arabes unis – et un réseau basé aux Émirats arabes unis impliqué dans la fourniture de biens pour le programme de missiles balistiques de l'Iran.

41. Ce réseau a dissimulé l'utilisateur final de produits sensibles pour la prolifération des missiles en utilisant des entreprises de façade dans des pays tiers pour tromper les fournisseurs étrangers. Il avait également désigné cinq personnes iraniennes qui ont travaillé pour obtenir des composants de missiles balistiques pour l'Iran. Hossein Pournaghshband et sa société, Mabrooka Trading, apportaient ou tentaient d'apporter un soutien financier, matériel, technologique ou autre à Navid Composite Material Company (Navid Composite), une entité également sanctionnée par les États-Unis dans le cadre du programme de missiles balistiques de l'Iran.

42. Au moment de sa désignation, Navid Composite concluait un contrat avec des entités asiatiques afin d'acheter une ligne de production de fibres de carbone pour produire des fibres de carbone adaptées à une utilisation dans les composants de missiles balistiques. Depuis au moins début 2015, Pournaghshband a fait appel à Mabrooka Trading pour s'approvisionner en matériaux et autres équipements pour le plan de production de fibres de carbone de Navid Composite. M. Pournaghshband est également désigné comme ayant apporté ou tenté d'apporter un soutien financier, matériel, technologique ou autre à Mabrooka Trading.

Cyberattaques

Étude de cas 1 : Attaque sur les bureaux d'échange de cryptomonnaies

43. Les auteurs de cyberattaques de la Corée du Nord se sont concentrés sur le ciblage des échanges de cryptomonnaies en 2019. Certains échanges de cryptomonnaies ont fait état de plusieurs attaques, en particulier celles enregistrées en Corée du Sud. La société Bithumb aurait été attaquée par des Nord-Coréens au moins quatre fois. Les deux premières attaques, survenues en février et juillet 2017, ont entraîné des pertes d'environ 7 000 000 USD chacune, les attaques ultérieures en juin 2018 et mars 2019 ayant entraîné une perte de 51 000 000 USD. De même, Youbit (anciennement Yapizon) a subi de multiples attaques impliquant une perte de 4,8 millions USD en avril 2017 puis 17 % de son actif global en décembre 2017, forçant la clôture de l'échange.

Étude de cas 2 : Attaque ciblant des institutions financières

44. Les enquêtes ont révélé des éléments probants à l'appui des cyberattaques menées par la Corée du Nord qui volent les fonds des IF de différents pays, ce qui a permis à la Corée du Nord d'échapper aux sanctions financières et de générer des revenus qu'il est plus difficile de retrouver et qui font l'objet d'une surveillance et d'une réglementation gouvernementales moins importantes. En 2019, des enquêtes ont été menées auprès d'au moins 35 affaires signalées de ressortissants de la Corée du Nord impliqués dans l'attaque d'institutions financières dans le but d'obtenir des devises étrangères, entre autres, de Malte, du Koweït, de l'Afrique du Sud, du Vietnam, de la Pologne, de la Slovénie et du Chili.

45. Selon le Groupe d'experts des Nations Unies, ces attaques ciblées se sont considérablement renforcées en termes de portée et de sophistication, les fonds acquis illégalement par la Corée du Nord étant estimés à jusqu'à 2 000 000 000 USD.

SIGNAUX D'ALARME LIES AU FP

46. Ci-après figure une liste non exhaustive d'éventuels signaux d'alarme liés au FP qui peuvent aider les IF et les EPNFD à détecter toute opération suspecte relative au FP[5]:

- La transaction implique une personne ou une entité située dans un pays étranger concerné par la prolifération.
- L'opération implique une personne ou une entité située dans un pays étranger concerné par le détournement.
- Le client ou la contrepartie ou son adresse est similaire à l'une des parties figurant sur les listes publiques de « personnes refusées » ou à un historique d'infractions au contrôle des exportations.
- Une entreprise de transport est indiquée comme destination finale du produit.
- La commande de biens est passée par des entreprises ou des personnes de pays étrangers autres que le pays de l'utilisateur final déclaré.
- La transaction implique d'éventuelles sociétés-écrans (par exemple, les sociétés ne disposent pas d'un niveau élevé de capitalisation ou affichent d'autres indicateurs de sociétés-écrans).
- La transaction démontre des liens entre les représentants d'entreprises échangeant des biens, c'est-à-dire les mêmes propriétaires ou la direction.
- Itinéraire d'expédition indirect (le cas échéant) et/ou Itinéraire de transaction financière indirect.
- La transaction concerne des personnes ou des sociétés (notamment des sociétés commerciales) situées dans des pays dont le contrôle des exportations est médiocre, tout comme leur application des lois sur le contrôle des exportations.
- La transaction implique l'expédition de biens incompatibles avec les mécanismes commerciaux géographiques normaux (par exemple, le pays concerné exporte/importe normalement le(s) bien(s) concerné(s)).
- D'après la documentation obtenue dans le cadre de la transaction, la valeur déclarée de l'expédition a manifestement été sous-évaluée par rapport au coût d'expédition.
- Incohérences dans les informations contenues dans les documents commerciaux et les flux financiers, tels que les noms, les sociétés, les adresses, la destination finale, etc.
- Les instructions de virement ou le paiement par des parties non identifiées dans la lettre de crédit originale ou toute autre documentation.
- Participation d'articles contrôlés en vertu des régimes de contrôle des exportations des ADM ou des régimes de contrôle nationaux.
- L'implication d'une personne liée à un pays concerné par la prolifération (par exemple, une double nationalité) et/ou qui traite d'équipements complexes au sujet desquels elle ne dispose pas de connaissances techniques.
- Les clients ou contreparties à des transactions sont liés (par exemple, ils partagent une adresse physique commune, une adresse IP ou un numéro de téléphone, ou leurs activités peuvent être coordonnées).
- Participation d'une université dans un pays concerné par la prolifération.
- La description des biens figurant sur le marché ou la documentation financière est non spécifique, banale ou trompeuse.
- La preuve que les documents ou autres déclarations (par exemple relatifs à l'expédition, aux douanes ou au paiement) sont faux ou frauduleux.
- Utilisation d'un compte personnel pour acheter des articles industriels.

[5] « Recommandations sur la lutte contre le financement de la prolifération – Mise en œuvre des dispositions financières des résolutions du Conseil de sécurité des Nations Unies visant à lutter contre la prolifération des armes de destruction massive – Rapport sur le financement de la prolifération », GAFI, 2018