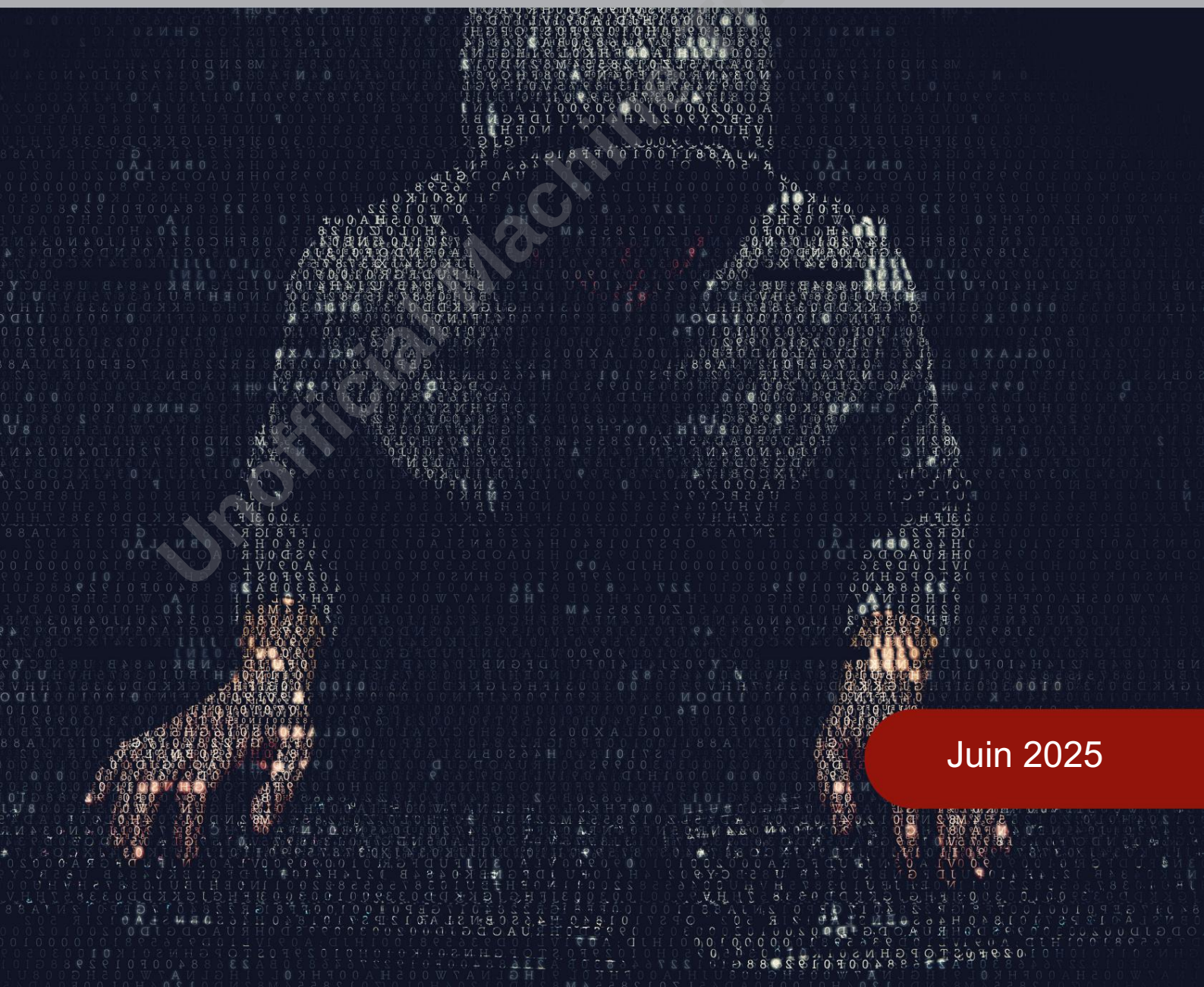
FATF

Rapport du GAFI

Systèmes complexes de financement de la prolifération et d'évasion des sanctions



Juin 2025

Le Groupe d'action financière (GAFI) est un organisme intergouvernemental indépendant qui élabore et promeut des politiques visant à protéger le système financier mondial contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive. Les recommandations du GAFI sont reconnues comme la norme mondiale en matière de lutte contre le blanchiment de capitaux (LAB) et le financement du terrorisme (FT).

Pour plus d'informations sur le GAFI, veuillez visiter www.fatf-gafi.org

Ce document et/ou toute carte qu'il contient sont sans préjudice du statut ou de la souveraineté de tout territoire, de la délimitation des frontières et limites internationales et du nom de tout territoire, ville ou zone.

Référence de citation :

GAFI (2025), Systèmes complexes de financement de la prolifération et d'évasion des sanctions, GAFI, Paris,
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/proliferation-complexe-financement-sanctions-evasion-schemes.html

Abréviations et acronymes

LBC/FT Lutte contre le blanchiment d'argent et le financement du terrorisme

Cryptomonnaies améliorant l'anonymat des AEC

Système d'identification automatisé AIS

APT38 Menace persistante avancée 38

Informations sur la propriété effective ultime de l'UBOI

Monnaie numérique de la banque centrale CBDC

Diligence raisonnable à l'égard de la clientèle en matière de CDD

Financement de la lutte contre la prolifération du CPF

CVC, monnaie virtuelle convertible

DeFi Finance décentralisée

Entreprise et profession non financière désignées DNFBP

RPDC République populaire démocratique de Corée

Diligence raisonnable renforcée EDD

Institutions financières internationales

FTB Banque du commerce extérieur

Zones franches (FTZ)

Coalition mondiale pour le contrôle des exportations (GECC)

OMI Organisation maritime internationale

Note interprétative de la recommandation de l'INR

Corps des gardiens de la révolution islamique (CGRI)

Blanchiment d' argent /Financement du terrorisme

Service de transfert d'argent ou de valeur MVTS

Évaluation nationale des risques de la NRA

OTC en vente libre

Financement de la prolifération du PF

Groupe d'experts du PoE

P2P pair à pair

PPP Partenariats public-privé

Bureau général de reconnaissance du RGB

Rapport d'activité/transaction suspecte SAR/STR

Organisme d'autorégulation SRB

TCSP Fournisseur de services de fiducie et d'entreprise

Sanctions financières ciblées du TFS

ONU Nations Unies

Conseil de sécurité des Nations Unies

Résolution du Conseil de sécurité des Nations Unies

VASP Fournisseur de services d'actifs virtuels

ADM Armes de destruction massive

1. Résumé

La prolifération des armes de destruction massive (ADM) et le financement qui y est associé représentent une menace importante pour la sécurité mondiale et l'intégrité du système financier international. Si la conformité technique et l'efficacité ne sont pas renforcées par les secteurs public et privé, des acteurs étatiques et non étatiques sophistiqués continueront de profiter des faiblesses des contrôles du dispositif de lutte contre le financement de la prolifération (PCF). L'impact potentiellement catastrophique des ADM rend cruciale la prévention et la lutte contre le financement de cette activité illicite.

Les systèmes complexes de financement de la prolifération (PF) et de contournement des sanctions constituent des menaces majeures pour le système financier international. Conformément au mandat du GAFI, ce rapport met en lumière les méthodes et tendances pertinentes et appuie les évaluations des menaces et des risques aux niveaux national, régional et mondial. L'étude détaille les techniques utilisées par ceux qui contournent les sanctions financières ciblées (SFC) liées au PF, décrites dans la Recommandation 7, exigée par les Normes du GAFI, ainsi que les techniques permettant de contourner d'autres régimes de sanctions (tels que les sanctions nationales et supranationales) qui ne sont pas couvertes par la Recommandation 7 des Normes du GAFI.

Cette approche globale vise à fournir une compréhension actualisée des menaces et des vulnérabilités, y compris des défis communs aux typologies concernées. L'étude s'efforce également d'identifier les principaux défis en matière d'application de la loi et les bonnes pratiques, qui
contribue à éclairer les évaluations des risques liés aux sanctions financières des pays et leurs processus d'atténuation. Le cadre plus large de l'évasion des sanctions ne vise pas à redéfinir les exigences de la recommandation 7, et n'implique ni ne favorise l'adoption de régimes de sanctions nationaux ou supranationaux.[1]

Le GAFI estime que l'évolution des menaces et des vulnérabilités liées au financement du terrorisme et au contournement des sanctions représente un défi majeur pour les secteurs public et privé. Le contexte de risque actuel est caractérisé par l'acquisition et/ou l'approvisionnement de biens, de technologies et de connaissances à double usage par des acteurs étatiques et non étatiques via des réseaux d'approvisionnement. Compte tenu de la menace mondiale actuelle liée au financement du terrorisme, le Réseau mondial du GAFI a reconnu la République populaire démocratique de Corée (RPDC) comme l'acteur le plus important. La RPDC est soumise aux sanctions de l'ONU et aux normes du GAFI.

Bien qu'il n'existe pas d'estimation universellement reconnue du montant total des fonds générés ou transférés pour soutenir le PF, la RPDC a diversifié ses efforts pour accéder au système financier et générer des revenus pour son programme d'armes de destruction massive ces dernières années. Par exemple, la RPDC a généré des milliards de dollars grâce à des cyberattaques contre des entreprises liées aux actifs virtuels, comme le vol de 1,5 milliard de dollars à ByBit en février 2025. Par ailleurs, la RPDC génère des revenus grâce aux informaticiens, à divers autres secteurs et à des activités illicites au profit de son programme d'armes de destruction massive.

De nombreux pays ont également identifié des exemples pertinents de stratagèmes visant à contourner les sanctions, impliquant l'Iran et la Fédération de Russie, qui ne sont pas soumis aux sanctions de l'ONU liées à la prolifération ni couverts par la définition du risque de PF du GAFI. Compte tenu de la diversité des niveaux de compréhension des risques, les acteurs malveillants exploitent avec succès les vulnérabilités nationales et sectorielles pour échapper aux sanctions relatives à la PF (voir section I).

1. Le cadre plus large de l'évasion des sanctions ne crée aucune nouvelle obligation liée à la Recommandation 1 ou à toute autre partie des Normes du GAFI. Les rapports de typologie du GAFI visent plutôt à aider les secteurs public et privé à évaluer et à atténuer les risques en fonction de leur contexte spécifique.

Les acteurs illicites recourent à des stratagèmes sophistiqués pour échapper aux sanctions et contourner les contrôles à l'exportation relatifs au PF. S'appuyant sur les informations soumises par le Réseau mondial du GAFI, ce rapport met en lumière quatre typologies majeures : le recours à des intermédiaires pour échapper aux sanctions ; la dissimulation des informations sur la propriété effective (BOI) pour accéder au système financier ; l'utilisation d'actifs virtuels et d'autres technologies ; et l'exploitation des secteurs maritime et du transport maritime (voir section II). Pour lutter contre les stratagèmes complexes de PF et d'évasion des sanctions, le rapport présente les défis et les bonnes pratiques en matière de : détection du PF et d'évasion des sanctions ; enquêtes et poursuites ; coordination et collaboration nationales ; et coopération internationale (voir section III).

Cette étude contribue à la compréhension par le Réseau mondial du GAFI des schémas complexes de fraude fiscale et de contournement des sanctions, notamment grâce à des indicateurs de risque pertinents pour les autorités compétentes et le secteur privé (voir Annexe A : Indicateurs de risque). Cependant, cette étude souligne également la nécessité d'améliorer encore la compréhension collective du Réseau mondial du GAFI des risques liés à la fraude fiscale et au contournement des sanctions. Dans les années à venir, les acteurs malveillants continueront de sonder les faiblesses des contrôles du CPF, telles que les différences juridictionnelles dans l'approche de la fraude fiscale et du contournement des sanctions, et d'exploiter les nouvelles technologies et les évolutions du paysage géopolitique.

Pour prévenir et combattre les systèmes complexes d'évasion fiscale et de sanctions, le GAFI mondial
Le réseau devrait prendre en compte (voir la section Recommandations) :

1) Mettre à jour périodiquement la compréhension des menaces, des vulnérabilités et des typologies, étant donné que les secteurs public et privé sont à des stades différents de compréhension des risques pertinents ;

2) Encourager un partage d'informations plus substantiel pour renforcer la capacité des secteurs public et privé à détecter les cas de fraude fiscale et/ou d'évasion des sanctions, compte tenu du recours aux SAR/STR pour lancer les enquêtes pertinentes ;

3) Ajouter une définition officielle des ADM PF au Glossaire général du GAFI, dans un délai de cinq ans, afin de surmonter les différences juridictionnelles qui compromettent la coopération internationale ; et

4) Réaliser un examen horizontal des évaluations des risques de FP du Réseau mondial du GAFI, dans un délai de trois ans, afin de contribuer à identifier les bonnes pratiques une fois que les pays auront eu plus de temps pour évaluer les risques de FP.

2. Contexte

Aperçu des normes du GAFI et des travaux sur le PF

1. En octobre 2020, le GAFI a adopté des amendements aux Recommandations 1 et 2 (R.1 et R.2) et à leurs Notes interprétatives (INR.1 et INR.2) afin d'exiger des pays, des institutions financières, des entreprises et professions non financières désignées (EPNFD) et des prestataires de services d'actifs virtuels (PSAV) qu'ils identifient, évaluent et comprennent leurs risques de financement de la prolifération, c'est-à-dire le risque de violation potentielle, de non-application ou d'évasion des sanctions financières ciblées (SFC) détaillées dans la R.7, et qu'ils prennent des mesures d'atténuation efficaces et proportionnées aux risques identifiés. Les Recommandations révisées obligent également les pays à renforcer la coopération et la coordination nationales, ainsi que les mécanismes de partage d'informations liés aux risques de PF.

2. Afin d'aider les acteurs des secteurs public et privé à mettre en œuvre efficacement les obligations découlant des Recommandations révisées, le GAFI a publié en 2021 le Guide sur l'évaluation et l'atténuation des risques liés au financement de la prolifération2, qui fournit des orientations sur :

1) comment les secteurs public et privé devraient mener des évaluations des risques pour identifier, évaluer et comprendre les risques liés aux PF ;
2) comment mettre en œuvre les exigences du GAFI pour atténuer les risques identifiés liés aux PF ; 3) comment les superviseurs ou les organismes d'autorégulation devraient superviser et surveiller les IF, les EPNFD et les PSAV pour s'assurer qu'ils évaluent et atténuent correctement les risques liés aux PF.

3. Les Orientations de 2021 complètent les Orientations de 2018 sur le financement de la lutte contre la prolifération3, qui visent principalement à aider les acteurs des secteurs public et privé à comprendre et à mettre en œuvre les obligations découlant de la R.7 des résolutions du Conseil de sécurité des Nations Unies, ainsi qu'à prévenir le contournement des sanctions. Elles sont précédées des Orientations de 2013 sur la 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 massive4 .

4. Avant ces documents d'orientation, le GAFI a identifié et analysé les risques existants liés au financement de la prolifération et les mesures du CPF et a publié les conclusions dans le Rapport sur les typologies du financement de la prolifération de 20085 afin de mieux comprendre ces évolutions à l'échelle mondiale. Le rapport de 2010 intitulé « Lutte contre le financement de la prolifération : Rapport d'étape sur l'élaboration des politiques et la consultation »6 s'appuie sur le rapport de 2008 en présentant les options politiques à prendre en compte dans la mise en œuvre des mesures du CPF conformément aux résolutions du Conseil de sécurité des Nations Unies, notamment en ce qui concerne i) les systèmes juridiques, ii) le partage d'informations et sensibilisation entre les secteurs public et privé, iii) mesures préventives et iv) enquêtes et poursuites.

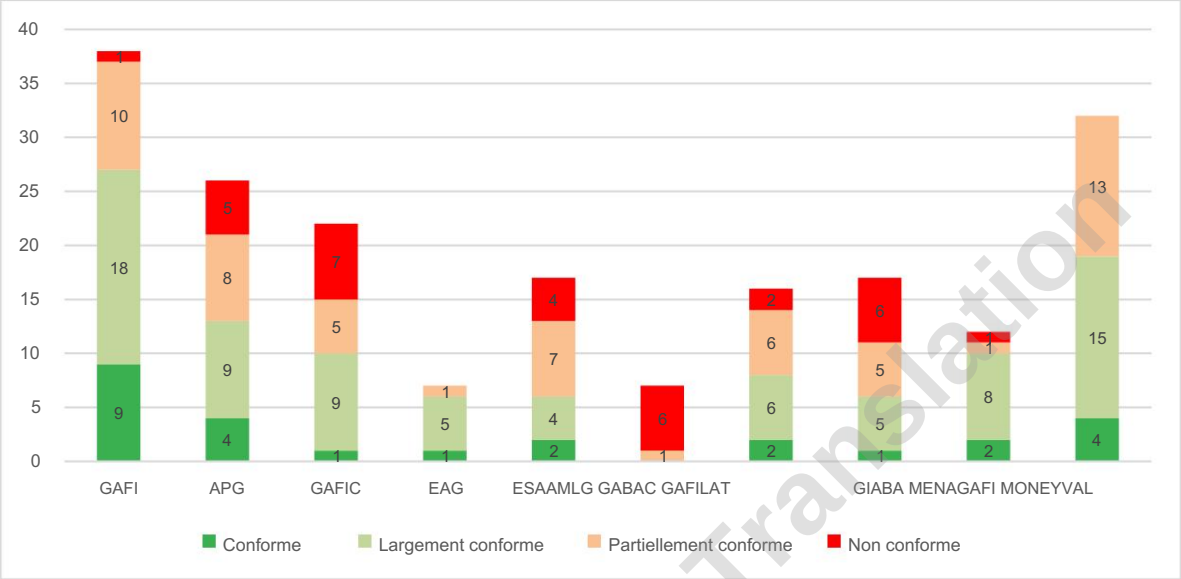
État actuel de mise en œuvre des normes du GAFI

5. Les résultats du quatrième cycle d'évaluation mutuelle (EM) indiquent que les pays continuent de rencontrer des difficultés avec la recommandation 7 et la mise en œuvre et l'application de la TFS conformément aux résolutions du Conseil de sécurité des Nations Unies sur la prolifération. En avril 2025, , sur 194 membres du GAFI et du FSRB

2 GAFI (2021) Orientations sur l'évaluation et l'atténuation des risques liés au financement de la prolifération.
3 GAFI (2018) Orientations sur la lutte contre le financement de la prolifération 4 GAFI (2013) Orientations sur la mise en œuvre des dispositions financières des résolutions du Conseil de sécurité des Nations Unies pour lutter contre la prolifération des armes de destruction massive
5 Rapport du GAFI (2008) sur les typologies de financement de la prolifération
6 GAFI (2010) Lutte contre le financement de la prolifération : rapport d'étape sur l'élaboration des politiques et Consultation
7 notes d'évaluation consolidées du GAFI (2024)

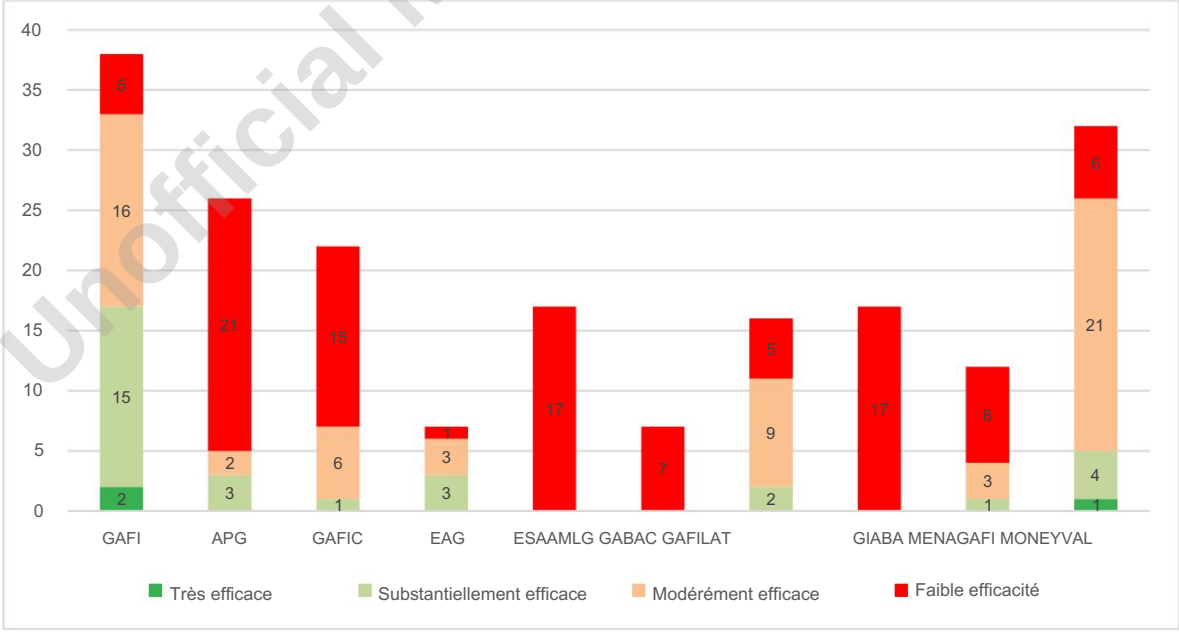
évalués lors du 4ème cycle de ME, seulement 13% (26 pays) sont conformes à la R.7 et près de la moitié (46% ; 89 pays) sont partiellement ou pas conformes.

Figure 1. Résultats de l'évaluation : Conformité technique avec la norme R.7 (en avril 2025)



6. De même, l'efficacité globale reste faible, avec seulement 16 % des pays évalués ayant démontré une efficacité élevée/substantielle dans l'IO.11 (TFS conformément aux résolutions du Conseil de sécurité des Nations Unies sur la prolifération). Les performances en matière d'efficacité varient considérablement entre les membres du GAFI et de l'ORGS (45 % des 38 membres du GAFI et 10 % des 156 membres de l'ORGS évalués ont obtenu des notes d'efficacité élevée/substantielle).

Figure 2. Résultats de l'évaluation : Résultat immédiat 11 – Efficacité (en avril 2025)



Introduction

Aperçu de Focus

7. Ce rapport vise à s'appuyer sur les deux rapports d'orientation existants et à les mettre à jour : 1) 2018 Orientations du GAFI sur la lutte contre le financement de la prolifération – Mise en œuvre des dispositions financières de la résolution 1718 du Conseil de sécurité des Nations Unies pour lutter contre les armes de destruction massive et 2) Orientations de 2021 sur l'évaluation et l'atténuation des risques liés au financement de la prolifération. Cette étude offre aux lecteurs une compréhension approfondie des typologies actuelles des schémas complexes de contournement des sanctions.
Il identifie les enjeux liés à la protection des données et les meilleures pratiques en matière d'application de la loi, contribuant ainsi à éclairer l'évaluation et l'atténuation des risques liés à la protection des données par les pays. Le rapport utilise les éléments clés suivants : termes:

Encadré 1. Définitions des termes clés

Le rapport utilise les définitions de travail générales utilisées dans les orientations PF 2021, qui s'appuient sur le rapport d'étape 2010 :

Prolifération des armes de destruction massive (ADM)

La fabrication, l'acquisition, la possession, le développement, l'exportation, le transbordement, le courtage, le transport, le transfert, le stockage ou l'utilisation d'armes nucléaires, chimiques ou biologiques et de leurs vecteurs et des matières connexes (y compris les technologies à double usage et les biens à double usage utilisés à des fins non légitimes).

Financement de la prolifération (PF)

Collecter, déplacer ou mettre à disposition des fonds, d'autres actifs ou d'autres ressources économiques, ou financer, en tout ou en partie, des personnes ou des entités à des fins de prolifération d'armes de destruction massive, y compris la prolifération de leurs vecteurs et des matériaux connexes (y compris les technologies à double usage et les biens à double usage à des fins non légitimes).8

Le rapport réitère qu'il n'existe pas de définition standard et universelle de la prolifération des armes de destruction massive ou de la PF partagée par les régimes et forums internationaux compétents et note les implications potentielles et la nécessité d'une définition standard dans les sections pertinentes.

Risques liés au PF

Sauf indication contraire, conformément à la Recommandation 1 révisée et à sa Note interprétative (R.1 et INR.1), le rapport fait référence au risque PF strictement et uniquement comme étant la violation potentielle, la non-mise en œuvre ou l'évasion des obligations TFS visées dans la Recommandation 7.

S'appuyant sur le vaste corpus de travaux de diverses institutions nationales et internationales, le rapport est conçu pour être utilisé par les membres du réseau mondial du GAFI,

8 Cette définition pratique du financement du terrorisme s'appuie sur celle du Rapport de situation 2010 du GAFI, qui reste pertinente pour la présente étude, notamment pour les pays adoptant une approche plus large de l'atténuation des risques liés au financement du terrorisme et au contournement des sanctions. Le rapport de 2010 définit le financement du terrorisme comme « le fait de fournir des fonds ou des services financiers utilisés, en tout ou en partie, pour la fabrication, l'acquisition, la possession, le développement, l'exportation, le transbordement, le courtage, le transport, le transfert, le stockage ou l'utilisation d'armes nucléaires, chimiques ou biologiques et de leurs vecteurs et des matières connexes (y compris les technologies et les biens à double usage utilisés à des fins illicites), en violation des lois nationales ou, le cas échéant, des obligations internationales ».

autorités compétentes, institutions financières, entreprises et professions non financières désignées, prestataires de services financiers virtuels, organisations non gouvernementales et toute autre personne ou organisme dans la lutte contre les évasions de sanctions concernant les PF.

Objectifs et structure

Ce rapport vise à fournir une vue d'ensemble des tendances et des méthodes de contournement des sanctions concernant le financement du terrorisme, afin d'aider les pays à atténuer les risques liés au financement du terrorisme. Il fournit des indicateurs des schémas complexes de contournement des sanctions, des menaces et des vulnérabilités, et identifie les bonnes pratiques et les défis en matière de détection, d'enquête et de poursuite des cas de contournement des sanctions concernant le financement du terrorisme. Ces objectifs sont atteints en quatre parties principales :

- Section 1 : Définit la portée du projet conformément au plan de mise en œuvre.
  Il fournit également un aperçu de la situation actuelle et identifie les menaces et les vulnérabilités liées à l'évasion des sanctions et au PF sur la base d'études de cas et d'analyses de la littérature.

- Section deux : Fournit un aperçu des typologies des schémas complexes d'évasion des sanctions pertinents pour le PF.

- Troisième partie : Identifie les défis et les bonnes pratiques en matière de détection, de signalement, d'enquête et de poursuite des infractions liées au financement du terrorisme. Elle décrit également les différents mécanismes de coordination et de collaboration nationales et internationales pertinents à ce sujet.

- Conclusion et domaines prioritaires : résume le paysage global de la fraude fiscale et de l'évasion des sanctions et identifie les domaines dans lesquels des travaux supplémentaires sont nécessaires.

- Indicateurs de risque : Cette annexe est conçue pour améliorer la capacité des entités des secteurs public et privé à identifier les transactions et/ou activités suspectes associées aux programmes pertinents d'évasion fiscale et de sanctions.

Méthodologie

10. La méthodologie comprenait un examen et un affinement des matériaux existants disponibles sur les risques liés aux PF et aux PF, qui comprenaient :

- Une revue de la littérature pour identifier les tendances évolutives dans la nature et la portée des
  Les contournements des sanctions concernant le Front Polisario, notamment ceux issus des récents rapports du Groupe d'experts de la résolution 1718 du Conseil de sécurité des Nations Unies (POE). Cet examen s'est concentré sur les menaces, les vulnérabilités, ainsi que les tendances et méthodes émergentes.

- Une demande aux membres du Réseau mondial du GAFI de fournir des informations sur le contournement des sanctions concernant le PF. Cela comprenait a) des documents sur les produits de renseignement stratégique ou des études de cas fournissant des informations sur les typologies et les cas de contournement des sanctions concernant le PF ; b) les menaces et les vulnérabilités identifiées dans les évaluations des risques et les mesures d'atténuation ; c) les mécanismes de détection, d'enquête et de partage d'informations ; et d) les bonnes pratiques et les défis.

- Outre les indicateurs de risque soumis par les membres du Réseau mondial du GAFI, les rapports supplémentaires suivants ont également été examinés : i) les orientations sur l'évaluation des risques des FP par d'autres organisations et institutions, ii) les études sur les typologies des FP et iii) les orientations sur les TFS publiées par les pays.

- Le secteur privé, la société civile et le monde universitaire ont été encouragés à répondre à plusieurs questions lors d'une consultation publique pour éclairer le rapport, notamment en ce qui concerne les défis et les bonnes pratiques en matière de coordination et de collaboration nationales.

3. Section 1. Évasion des sanctions concernant le PF – Situation actuelle, menaces et vulnérabilités

Portée

Encadrement du rapport

11. Dans le cadre du processus d'évaluation des risques, les pays prennent en compte les risques de blanchiment d'argent (BA), de financement du terrorisme (FT) et de PF qui surviennent lorsqu'une menace pertinente exploite avec succès une vulnérabilité pour produire une conséquence. Selon le Réseau mondial du GAFI , la menace la plus importante que représentent les PF pour le système financier international est posée par les acteurs parrainés ou affiliés à un État, y compris, mais sans s'y limiter, ceux associés à l'évasion des sanctions et aux activités de PF liées à la RPDC, le seul pays sanctionné par l'ONU.

12. Dans le cadre de la recommandation 1 révisée du GAFI, le risque de PF se réfère strictement et uniquement à la violation potentielle, à la non-application ou au contournement des obligations TFS visées dans la recommandation 7, qui se concentre uniquement sur le pays sanctionné par l'ONU, la RPDC.
Sur la base de cette définition étroite du risque de PF couvert par les normes du GAFI, les principaux acteurs de la menace identifiés par les juridictions comprennent la RPDC et les acteurs étatiques, les individus et les entités qui soutiennent ou travaillent avec la RPDC pour échapper aux sanctions de l'ONU.

13. Comme décrit dans les Lignes directrices 2021 du GAFI sur les FP10, une compréhension du risque plus large de prolifération des ADM et de son financement sous-jacent peut contribuer à la compréhension du risque lié aux obligations du GAFI en matière de FP-SFT. Une meilleure compréhension du risque lié aux FP peut également faciliter la mise en œuvre de mesures fondées sur le risque et de SFT. De nombreux membres du GAFI utilisent une définition plus large des FP afin d'atténuer le risque de manière plus large que les normes actuelles du GAFI.
Par conséquent, la portée des observations des juridictions reflétait leur compréhension de la menace mondiale actuelle que représente le PF, y compris la RPDC (soumise aux sanctions de l'ONU et aux normes du GAFI), mais aussi d'autres acteurs étatiques. De nombreux pays ont identifié l'Iran et la Fédération de Russie comme des menaces actuelles liées au PF, même s'ils ne sont pas soumis aux sanctions de l'ONU liées à la prolifération ni couverts par la définition du risque de PF du GAFI.

14. Ce rapport a pour objectif de fournir une vue d'ensemble actualisée des mécanismes complexes de contournement des sanctions utilisés par les financiers de la prolifération et, le cas échéant, d'examiner plus largement les mécanismes de contournement des sanctions liés au FT et au PF, quel que soit le régime de sanctions, afin de garantir la pérennité et la validité des typologies obtenues et de relever les défis communs. Par conséquent, ce rapport couvre tous les acteurs les plus cités par les juridictions afin d'aider le Réseau mondial du GAFI à identifier et à atténuer son risque de PF.
[11]

L'expérience du réseau mondial du GAFI dans l'évaluation des risques liés aux PF

15. Une méthode efficace pour évaluer les vulnérabilités pertinentes consiste à réaliser une évaluation des risques liés aux FP. La plupart des pays du réseau mondial du GAFI ont déclaré avoir

---

9 GAFI (2024) Guide national d'évaluation des risques liés au blanchiment d'argent 10 GAFI (2021) Orientations sur l'évaluation et l'atténuation des risques liés au financement de la prolifération 11 Comme indiqué dans le résumé et ailleurs dans le document, ce rapport inclut des informations sur les techniques utilisées pour contourner les régimes de sanctions nationaux et supranationaux afin de fournir une compréhension actualisée des menaces et des vulnérabilités, y compris les défis communs aux typologies pertinentes qui ne sont pas couvertes par la Recommandation 7 des Normes du GAFI. Le cadre plus large du contournement des sanctions ne vise pas à redéfinir les exigences de la Recommandation 7.

Bien que les pays aient évalué ou soient en train d'évaluer les risques liés aux PF dans le cadre de leur processus national d'évaluation des risques, certains éléments indiquent que l'évaluation et/ou la compréhension des vulnérabilités liées aux PF n'en sont qu'à leurs débuts. Par exemple, près de la moitié des pays ayant répondu au questionnaire de ce rapport n'ont pas vérifié s'ils présentaient des vulnérabilités liées aux PF, tandis que six autres pays ont conclu qu'ils n'en présentaient aucune.

16. Dans certains cas, les pays ont indiqué un faible niveau de vulnérabilité au PF et à l'évasion des sanctions pour plusieurs raisons, notamment l'éloignement géographique des pays sanctionnés ; l'absence de relations diplomatiques ou commerciales avec les pays sanctionnés ; un secteur financier sous-développé avec une intégration limitée au marché financier mondial ; un mécanisme national solide pour la mise en œuvre des TFS liés au PF ; et aucun cas de PF identifié dans la juridiction.

17. Nombre de ces facteurs constituent des facteurs légitimes pour réduire le risque que les acteurs de la menace du PF exploitent les vulnérabilités nationales ou sectorielles. Il est néanmoins important de prendre en compte l'évolution considérable du contexte mondial ces dernières années, avec l'émergence de nouvelles technologies, notamment de nouveaux systèmes de paiement, et la montée des tensions géopolitiques. De plus, ces facteurs ne prennent pas en compte les faiblesses plus larges des contrôles de LBC/FT/CPF dans les secteurs public et privé, ni la prévalence des acteurs de la menace du PF et de l'évasion des sanctions qui utilisent divers intermédiaires dans des pays tiers pour contourner les sanctions et les contrôles à l'exportation (voir Typologie 1). Étant donné que les acteurs de la menace du PF prospèrent en exploitant les angles morts potentiels du système financier international, un soutien et des activités accrus pourraient être nécessaires pour identifier et atténuer les vulnérabilités du PF et renforcer l'effort collectif visant à les atténuer.

Situation actuelle

18. Malgré les régimes de sanctions internationaux, supranationaux et nationaux exhaustifs et les contrôles à l'exportation visant les programmes d'ADM, des acteurs soutenus par des États ou affiliés à des États mettent en œuvre avec succès des systèmes complexes d'acquisition et de génération de revenus pour soutenir les acteurs et/ou les activités des PF. En particulier, les principaux acteurs de la menace font appel à des intermédiaires dans des pays tiers, dissimulent les BOI, utilisent les nouvelles technologies et exploitent les secteurs maritime et du transport maritime pour échapper aux sanctions, lever des fonds et acquérir des biens à double usage. (voir section 2).

19. Le GAFI évalue les menaces et vulnérabilités actuelles comme suit :

Situation actuelle – RPDC

20. La RPDC est soumise à d'importantes sanctions internationales depuis que l'État a procédé à son premier essai nucléaire en 2006. La résolution 1718 du Conseil de sécurité des Nations Unies, adoptée en 2006, exigeait que la RPDC cesse ses essais nucléaires et mettait en place, entre autres contre-mesures, la TFS contre la RPDC en général, mais aussi contre des individus et des entités spécifiques associés au programme d'armes de destruction massive de la RPDC.

21. Bien que soumise à des sanctions de l'ONU depuis près de vingt ans, la RPDC continue de développer ses capacités à lancer un engin nucléaire grâce à des essais de missiles balistiques intercontinentaux. Par exemple, le 31 octobre 2024, la RPDC a lancé un ICBM baptisé Hwasong-19, qui a atteint une altitude d'environ 7 000 km et parcouru une distance totale d'environ 1 000 km. Ce dernier essai est le onzième lancement d'ICBM par la RPDC depuis l'annonce d'un nouveau plan quinquennal d'expansion militaire en 2021.

Le dernier tir de missile de la Corée du Nord constitue une « grave menace » pour la stabilité régionale | ONU Actualités

22. Bien que la RPDC ait poursuivi ces activités, l'action de la communauté internationale n'a pas suivi le rythme ni la trajectoire de la menace posée par le pays. Aucun ajout n'a été effectué à la liste des sanctions de l'ONU contre la RPDC depuis près de dix ans. De plus, le Groupe d'experts du Comité créé par la résolution 1718 du Conseil de sécurité des Nations Unies a été dissous en 2024. Cette dissolution représente un défi majeur pour le suivi des violations des sanctions visant la RPDC.13 De nombreux pays se sont appuyés sur les rapports semestriels du Groupe d'experts de la résolution 1718 du Conseil de sécurité des Nations Unies pour éclairer leurs évaluations nationales des risques liés au financement du terrorisme. Comme l'a souligné la plénière du GAFI en juin 2024, « la capacité d'obtenir des informations fiables et crédibles pour étayer l'évaluation des risques liés au financement du terrorisme en RPDC est entravée par la récente cessation du mandat du Groupe d'experts du Comité créé par la résolution 1718 ».14

23. Lors de la réalisation de cette étude, les délégations du GAFI ont soulevé deux principaux facteurs aggravants contribuant au financement du programme d'armes de destruction massive de la RPDC : la connectivité financière croissante du pays et la diversité de ses sources de revenus.

Accroître la connectivité financière de la RPDC

de 24. Alors que le GAFI a continuellement réitéré depuis 2011 la nécessité pour tous les pays de mettre en œuvre manière rigoureuse des TFS conformes aux résolutions du Conseil de sécurité de l'ONU et d'appliquer des contre-mesures pour protéger leur système financier contre les financements illicites émanant de la RPDC, la juridiction a récemment accru sa connectivité avec le système financier international, ce qui augmente les risques de PF, comme le GAFI l'a également noté en juin 2024.15

25. Dans le Traité de partenariat stratégique global entre la RPDC et la Russie16, entré en vigueur fin 2024, les deux pays s'engagent à renforcer leur coopération, notamment en créant des conditions favorables à la coopération économique dans les domaines financier et bancaire ; en collaborant pour créer des conditions favorables à l'établissement de liens directs entre la RPDC et la Fédération de Russie ; et en promouvant la compréhension mutuelle du potentiel économique et d'investissement des régions. Le renforcement des liens économiques, notamment par le rétablissement des relations bancaires avec les institutions financières de la RPDC ou les entités liées au PF, pourrait introduire de nouvelles vulnérabilités dans le système financier mondial, car plusieurs institutions financières de la RPDC et leurs représentants à l'étranger sont visés par la résolution 1718 du Conseil de sécurité des Nations unies17.

26. Depuis 2016, le nombre de pays accueillant des banquiers de la RPDC est passé de 14 à quatre en raison de l'application des sanctions par le pays hôte et du retrait du personnel de la RPDC, le plus récemment d'Indonésie et de Libye fin 2023. Cependant, de 2023 à au moins mi-2024, des banquiers de la RPDC dans un pays voisin et en Russie ont facilité des transactions évaluées à des centaines de millions de dollars pour soutenir le commerce et la génération de revenus de la RPDC. À la mi-2024, plus de 50 représentants bancaires de la RPDC opéraient à l'extérieur du pays, malgré la résolution 2321 du Conseil de sécurité des Nations Unies exigeant que les pays hôtes les expulsent.18 De plus, la résolution 2270 du Conseil de sécurité des Nations Unies exige que les pays hôtes ferment les bureaux de représentation existants et interdit à la RPDC d'ouvrir ou d'exploiter de nouvelles succursales, filiales ou bureaux de représentation dans les États membres de l'ONU.

Le Conseil de sécurité ne parvient pas à prolonger le mandat du groupe d'experts chargé d'assister le Comité des sanctions sur la démocratie République populaire de Corée | Couverture des réunions et communiqués de presse

14 pays à haut risque font l'objet d'un appel à l'action - juin 2024 15 pays à haut risque faisant l'objet d'un appel à l'action - juin 2024 16 http://en.kremlin.ru/acts/news/75534 17 entités désignées par l'ONU comprennent la Tanchon Commercial Bank (KPe.003), la Bank of East Land (KPe.013), Amroggang Development Banking Corporation (KPe.009).

La résolution 2321 du Conseil de sécurité des Nations Unies exige que les pays hôtes prennent des mesures proactives, telles que l'expulsion des représentants bancaires de la RPDC et l'interdiction du soutien financier public et privé depuis leur territoire ou par des personnes ou entités soumises à leur juridiction pour le commerce avec la RPDC.

19 Une délégation a noté qu'en janvier 2024, un banquier basé en Russie a permis la conclusion d'un accord visant à envoyer des ouvriers du bâtiment de la RPDC en Russie, où ils gagnent des devises étrangères et permettent à la RPDC de continuer à contourner les sanctions de l'ONU .

La diversité des activités génératrices de revenus de la RPDC profite à ses armes de destruction massive Programme

27. De nombreux pays ont signalé que les activités criminelles les plus souvent associées aux stratagèmes de contournement des sanctions et de financement du terrorisme concernent la contrefaçon, la fraude, le vol (cyber) et le trafic d'armes, de drogue, d'espèces sauvages, la contrebande et d'autres biens. Des individus et entités liés à la RPDC se livrent à ce type d'activités illicites et exploitent des entreprises légitimes pour générer des revenus destinés au programme d'ADM, ciblant en particulier les pays ou les secteurs où les contrôles de LBC/FT/PCF sont faibles, voire inexistants, comme les nouvelles technologies et les secteurs maritime et maritime (voir typologies 3 et 4). Outre l'accent mis ces dernières années sur la génération de revenus par le recours aux informaticiens, la RPDC est également connue pour cibler divers secteurs ou activités illicites à cette fin, notamment :

- Secteur des perruques et des faux cils : Certains pays surveillent l'utilisation par la RPDC des exportations lucratives de perruques et de faux cils pour accroître ses finances et atténuer l'impact des sanctions internationales visant à limiter son programme d'armes stratégiques. Au premier semestre 2024, ces produits représentaient près de 60 % de l'ensemble des exportations de la RPDC vers un pays voisin.

  Pour produire ces produits, la RPDC importe des matières premières du même pays voisin pour fabriquer des produits semi-finis, que la RPDC renvoie ensuite aux entreprises pour le traitement final et l'exportation vers des pays tiers.
  Les sociétés commerciales qui produisent des perruques sont subordonnées à des entités figurant sur la liste de la résolution 1718 du Conseil de sécurité de l'ONU, ce qui suggère que les revenus tirés de ces perruques pourraient soutenir le programme d'armement stratégique de la RPDC. Bien que les sanctions de l'ONU n'interdisent pas aux entreprises d'acheter des perruques et des faux cils originaires de RPDC, les entreprises impliquées dans la production et l'achat des produits finis pourraient ignorer le lien avec les entités sanctionnées par l'ONU.

- Commerce illégal d'espèces sauvages : La majeure partie de l'approvisionnement du commerce illégal d'espèces sauvages par la RPDC provient de pays d'Afrique subsaharienne, compte tenu des liens historiques de nombre de ces pays avec la RPDC. Le commerce illégal d'espèces sauvages est un moyen peu risqué et très rentable pour la RPDC de se financer. Avec le déclin de la présence diplomatique de la RPDC en Afrique subsaharienne ces dernières années, ce canal pourrait devenir plus difficile à exploiter par le personnel diplomatique. En outre, certains pays partagent l'avis du RUSI selon lequel les citoyens de la RPDC opérant sous couverture en tant que ressortissants de pays tiers pourraient jouer un rôle plus important dans l'approvisionnement et le transport de ces articles dans les années à venir (par exemple, en se faisant passer pour des ressortissants de pays tiers).

19 Comme décrit dans la déclaration du GAFI de juin 2024 sur les juridictions à haut risque, « Le GAFI n'a cessé de réitérer depuis 2011 la nécessité pour tous les pays d'appliquer rigoureusement les sanctions financières ciblées conformément aux résolutions du Conseil de sécurité des Nations Unies et d'appliquer les contre-mesures suivantes pour protéger leurs systèmes financiers contre la menace de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération émanant de la RPDC : mettre fin aux relations de correspondance avec les banques de la RPDC ; fermer toutes les filiales ou succursales des banques de la RPDC dans leur pays ; et limiter les relations d'affaires et les transactions financières avec des personnes de la RPDC. » Malgré ces appels, la RPDC a renforcé sa connectivité avec le système financier international, ce qui augmente les risques de financement de la prolifération (FP), comme l'a noté le GAFI en février 2024. Cela exige une vigilance accrue et une mise en œuvre et une application renouvelées de ces contre-mesures contre la RPDC. Comme indiqué dans la résolution 2270 du Conseil de sécurité des Nations Unies, la RPDC a fréquemment recours à des sociétés écrans, des sociétés fictives, des coentreprises et des structures de propriété complexes et opaques dans le but de violer les sanctions. À ce titre, le GAFI encourage ses membres et tous les pays à appliquer « renforcer la diligence raisonnable à l'égard de la RPDC et sa capacité à faciliter les transactions en son nom. »

individus connus pour leur transit et leur destination en matière de trafic d'espèces sauvages pays).20

Situation actuelle – Iran

28. L'Iran a été initialement sanctionné par l'ONU en vertu de la résolution 1737 du Conseil de sécurité des Nations Unies après que le pays a refusé de se conformer à la résolution 1696 du Conseil de sécurité des Nations unies, qui exigeait que l'Iran cesse son programme d'enrichissement d'uranium. Cette résolution était la première d'une série imposant des TFS aux personnes et entités iraniennes liées à leur programme nucléaire.

29. Par la résolution 2231 du Conseil de sécurité des Nations Unies, le Conseil de sécurité a approuvé le Plan d'action global commun (PAGC), par lequel l'Iran a accepté de limiter son programme nucléaire en échange d'un allègement des sanctions et d'autres dispositions. Conformément à la résolution 2231 du Conseil de sécurité des Nations Unies, la TFS imposée aux personnes et entités liées au programme nucléaire iranien a pris fin en octobre 2023 et ne s'applique plus à la recommandation 7 du GAFI. Cependant, plusieurs pays utilisent des programmes nationaux de sanctions pour mettre en œuvre la TFS contre l'Iran en raison de la menace que représentent l'Iran et les personnes et entités qui lui sont affiliées.

L'Iran s'appuie sur des intermédiaires militarisés au Moyen-Orient ainsi que sur une trentaine d'organisations criminelles transnationales (OCT) basées en Iran et à l'étranger pour atténuer l'impact des sanctions économiques. Des hommes d'affaires étrangers bien connectés ont contribué aux activités de contrebande de pétrole iranien, tandis que les banques, les négociants en or et les bureaux de change peuvent servir d'intermédiaires importants pour le blanchiment d'argent et le contournement complexe des sanctions. Comme le montrent diverses études de cas, le contournement par l'Iran des sanctions et des contrôles à l'exportation peut favoriser le développement de missiles, d'armes, d'équipements aériens militaires et le programme d'armes de destruction massive.

Les intermédiaires de l'Iran ont bénéficié d'un accès à des marchés criminalisés, notamment les bureaux de change, qui servaient auparavant de relais de financement à Daech et à Al-Qaïda. Le Hezbollah a joué un rôle particulièrement important à cet égard, en raison de ses vastes opérations de contrebande, de son réseau mondial d'activités licites et illicites, et de son rôle dominant dans le blanchiment d'argent mondial par l'intermédiaire des bureaux de change. Le Hezbollah est lié à la contrebande de pétrole, d'armes et de diverses marchandises sanctionnées.

32. Le Hezbollah a également infiltré des institutions financières dans de nombreux pays et mené des opérations de blanchiment d'argent couvrant plusieurs continents et secteurs commerciaux. Des membres du Hezbollah ont même cherché à obtenir des armes et des équipements pour le compte de l'Iran, en violation des sanctions, une entreprise à haut risque. Ces relations montrent que les marchés criminels qui sous-tendent les opérations étrangères de l'Iran servent de catalyseurs à diverses menaces.

Situation actuelle – Russie

33. Suite aux sanctions internationales imposées à l'économie russe suite à l'invasion militaire de l'Ukraine, la Fédération de Russie a dû prendre des mesures pour soutenir son économie et sa position militaire. Comme indiqué précédemment, l'une de ces mesures comprend la signature du Traité de partenariat stratégique global avec l'Ukraine.

L' ONU enquête sur les allégations de trafic d'espèces sauvages en Corée du Nord en Afrique | NK News 21 Comme indiqué dans le résumé et ailleurs dans le document, ce rapport inclut des informations sur les techniques utilisées pour contourner les régimes de sanctions nationaux et supranationaux afin de fournir une compréhension actualisée des menaces et des vulnérabilités, y compris les défis communs aux typologies pertinentes qui ne sont pas couverts par la Recommandation 7 des Normes du GAFI. Le cadre plus large du contournement des sanctions ne vise pas à redéfinir les exigences de la Recommandation 7.

RPDC. 22 Ce traité crée des liens économiques et militaires entre les deux pays, y compris des dispositions visant à : renforcer la coopération stratégique et tactique ; fournir une assistance militaire ; et prendre des mesures conjointes pour renforcer les capacités de défense (voir paragraphe 26 pour des informations sur la coordination économique).

34. Français En avril 2025, la RPDC a confirmé le déploiement de soldats nord-coréens dans le conflit russo-ukrainien en vertu du traité bilatéral, tandis que les responsables russes ont confirmé les activités de soldats de la RPDC dans la région de Koursk.23 24 Auparavant, le rapport 1718 POE de l'ONU de mars 2024 citait les efforts de l'ONU pour enquêter sur la présence de munitions provenant de la RPDC en Ukraine.25 En raison de la connectivité économique et militaire entre la Russie et la RPDC, le principal acteur de la menace du PF sanctionné par l'ONU depuis deux décennies, de nombreux pays considèrent la Russie comme une menace du PF par extension.

Autres menaces

35. Français En outre, de nombreux pays restent préoccupés par les efforts déployés par des acteurs non étatiques, tels que des groupes terroristes et des organisations criminelles, pour acquérir et/ou se procurer des biens, des connaissances et des technologies liés aux ADM, y compris des capacités biologiques, chimiques et nucléaires. En novembre 2022, le Conseil de sécurité de l'ONU a renouvelé le mandat de la résolution 1540 du CSNU, en mettant l'accent sur la prévention de la prolifération des ADM, des connaissances ou des précurseurs vers des acteurs non étatiques.26 Comme indiqué dans les orientations 2021 du GAFI sur la prévention de la prolifération, les obligations de la résolution 1540 du CSNU existent séparément et indépendamment des obligations énoncées dans la recommandation 7 et sa note interprétative.27 Bien qu'il existe peu d'exemples d'acteurs non étatiques exploitant le système financier pour soutenir des acteurs ou des activités de PF, de nombreux pays considèrent que l'impact potentiel de ces activités justifie un suivi régulier. De plus, certaines typologies de ces activités peuvent être pertinentes pour comprendre et atténuer les risques généraux de PF et de contournement des sanctions. Par conséquent, ce rapport présente quelques études de cas d'acteurs non étatiques.

Vulnérabilités

36. Comme décrit dans les Lignes directrices 2021 du GAFI sur les FP, la vulnérabilité désigne les facteurs exploitables par la menace concernée ou les acteurs menaçants susceptibles de soutenir ou de faciliter la violation, la non-application ou le contournement des FP-TFS. Selon les normes existantes du GAFI, cela s'applique à la menace posée par la RPDC et les acteurs associés qui l'aident à se soustraire aux sanctions de l'ONU. Pour les pays qui envisagent le risque de FP sous un angle plus large, cela s'appliquerait aux vulnérabilités exploitées par tous les acteurs de FP cherchant à exploiter les faiblesses des secteurs public et privé.

37. Les pays devraient prendre en compte les vulnérabilités aux niveaux national (y compris structurel) et sectoriel. Une vulnérabilité nationale ou structurelle peut inclure des faiblesses dans le cadre juridique et réglementaire de la LBC/FT/CPF. D'autres vulnérabilités au niveau national peuvent inclure des facteurs inhérents à la juridiction, tels que la taille et la complexité de l'économie, le degré d'informalité/de liquidités de l'économie, ou la diversité des personnes morales et des arrangements. 28 Pour l'exposition aux vulnérabilités liées au FP en particulier, de nombreux pays.

22 http://kcna.kp/en/article/q/6a4ae9a744af8ecdfa6678c5f1eda29c.kcmsf 23 http://www.rodong.rep.kp/en/index.php?MTJAMjAyNS0wNC0yOS0wMDFAMTVAMUBAMEAxQA== 24 http://en.kremlin.ru/events/president/news/76805 25 https://docs.un.org/fr/S/2024/215 Le Conseil de sécurité prolonge de dix ans le mandat du Comité de surveillance des armes nucléaires, biologiques et chimiques , en adoptant à l'unanimité la résolution 2663 (2022) | Couverture des réunions et communiqués de presse 27 Orientations sur l'évaluation et l'atténuation des risques liés au financement de la prolifération 28 Guide national d'évaluation des risques liés au blanchiment d'argent 2024.pdf.coredownload.inline.pdf

Ils ont souligné l'importance de leur situation géographique. Ce facteur contextuel est identifié comme significatif dans son lien potentiel avec les plans de contournement des sanctions de la RPDC.

38. Une vulnérabilité sectorielle se rapporte aux caractéristiques propres à un secteur, susceptibles d'être exploitées abusivement par une personne ou une entité pour mettre en œuvre des schémas complexes de financement de la prolifération et de contournement des sanctions. Par exemple, les caractéristiques contextuelles du canal de distribution dans un secteur, telles que la prévalence d'intermédiaires et d'agents, peuvent entraver le suivi des flux financiers ou des mouvements d'actifs.

Vulnérabilités nationales en matière de fraude fiscale et d'évasion des sanctions

39. Certaines des vulnérabilités nationales les plus courantes, qui facilitent les schémas complexes de financement de la prolifération et d'évasion des sanctions, qui ont été identifiées par le Réseau mondial du GAFI sont les suivantes :

Facteurs économiques et commerciaux

40. De nombreux pays ont noté que les acteurs de la fraude fiscale et du contournement des sanctions ciblent les pays qui font office de centres financiers internationaux, compte tenu de leur importance pour les flux et les transports financiers mondiaux (voir Typologie 1). La vulnérabilité des fraudes fiscales découle de la vaste gamme de produits et de services offerts par les plateformes financières internationales, qui desservent une clientèle large et diversifiée. De plus, l'ouverture (notamment la présence de zones économiques spéciales)
La sophistication des systèmes financiers et économiques établis qui facilitent les transactions transfrontalières les rend particulièrement vulnérables aux abus des réseaux de prolifération illicite. Les pays dotés de ports stratégiques dotés d'infrastructures de transport et de logistique sont également susceptibles d'être utilisés à mauvais escient pour contourner les sanctions et les contrôles à l'exportation liés aux biens à double usage.

41. De plus, de nombreux pays ont cité des vulnérabilités liées au maintien de relations économiques et commerciales avec des pays sanctionnés 29, ce qui accroît l'exposition à d'éventuels stratagèmes de contournement des sanctions et du PF. L'alignement géopolitique, les dépendances ou les liens historiques peuvent créer des opportunités pour les acteurs de la menace du PF de cibler ces pays à l'insu de ces derniers afin de contourner les sanctions et d'accéder aux systèmes financiers et
ressources.

42. La plupart des pays ont souligné l'importance des services douaniers pour prévenir et détecter les schémas complexes d'évasion des sanctions concernant les PF. Les services douaniers jouent un rôle essentiel dans la collecte et l'échange d'informations aux niveaux national, régional et international (voir section 3).

Facteurs réglementaires

43. Bien que les pays aient progressé dans la mise en place d'une réglementation en matière de LBC/FT, la mise en œuvre mondiale des mesures liées au CPF accuse encore du retard (voir figures 1 et 2). En l'absence d'un cadre réglementaire, législatif et opérationnel solide, certains pays ne sont pas en mesure d'appliquer les obligations en matière de sanctions et de contrôles des exportations nécessaires pour dissuader et

29 Dans la pratique, de nombreux pays cherchent à remédier aux vulnérabilités liées au contournement des régimes de sanctions de l'ONU, nationaux et supranationaux. Cependant, la Recommandation 7 du GAFI ne s'applique qu'à la RPDC, qui est le seul pays sanctionné par l'ONU. Comme indiqué dans le résumé et ailleurs dans le document, ce rapport inclut des informations sur les techniques utilisées pour contourner les régimes de sanctions nationaux et supranationaux afin de fournir une compréhension actualisée des menaces et des vulnérabilités, y compris les défis communs aux typologies concernées qui ne sont pas couvertes par la Recommandation 7 des Normes du GAFI. Le cadre plus large du contournement des sanctions ne vise pas à redéfinir les exigences de la Recommandation 7.

Réseaux de lutte contre la prolifération. De plus, les stratagèmes complexes de fraude fiscale et de contournement des sanctions font appel à diverses techniques d'obscurcissement, encore plus difficiles à détecter dans les secteurs non réglementés ou insuffisamment surveillés, comme les PSAV. De plus, la vulnérabilité des PF est accrue dans les pays dont la législation nationale sur la transparence de la propriété effective des personnes morales est faible. La difficulté d'accès aux informations sur la propriété effective entrave les enquêtes transfrontalières menées par les autorités pour identifier et retracer la filière des PF, en particulier lorsque plusieurs pays sont concernés.
des cadres juridiques incohérents sont en jeu.

Facteurs géographiques et démographiques

44. Certains pays ont fait état de vulnérabilités liées à leur proximité géographique avec des pays soumis à des régimes de sanctions onusiens, nationaux et supranationaux, ce qui peut créer des opportunités pour les réseaux illicites de transférer des actifs et des ressources au-delà des frontières. Les pays stratégiquement situés offrent des voies de navigation et des routes commerciales vitales qui accroissent la vulnérabilité inhérente des pays voisins. Par exemple, les stratagèmes d'évasion des sanctions basés sur le commerce, impliquant la contrebande de marchandises illégales, sont plus susceptibles de se produire entre des pays proches d'une juridiction sanctionnée (voir Typologie 4). Comme le montrent les études de cas, les pays d'Asie de l'Est peuvent être exposés à la RPDC qui facilite des transactions financières et des expéditions détournées, tandis que les pays du Moyen-Orient peuvent créer des filières financières illicites pour le programme iranien d'armes de destruction massive. Par ailleurs, certains pays ont fait état de vulnérabilités liées à la présence de personnel diplomatique et d'autres acteurs concernés provenant de juridictions soumises à des régimes de sanctions onusiennes.

Autres facteurs au niveau national

45. Une autre vulnérabilité réside dans les volumes importants de devises étrangères largement utilisées, comme le dollar américain, dans le système financier mondial. Les pays doivent tenir compte des transactions transfrontalières effectuées dans ces devises, compte tenu de la vulnérabilité de l'utilisation de ces devises ou de comptes libellés dans ces devises à des fins d'achats illicites ou de contournement des sanctions.

46. De plus, les réseaux de prolifération cherchent à exploiter des facteurs industriels et technologiques pour acquérir illicitement des biens. Ainsi, les pays producteurs de technologies et de biens sensibles à la prolifération sont intrinsèquement vulnérables à la prolifération nucléaire et aux violations des restrictions sur les biens à double usage. Les pays dotés d'un important secteur de la défense ont besoin d'un nombre important d'organisations pour leur fournir des matériaux, des produits et des services. Cela offre aux réseaux de prolifération nucléaire l'opportunité de tirer parti de chaînes d'approvisionnement complexes.

de Enfin, les rapports POE de la résolution 1718 du Conseil de sécurité des Nations Unies ont souligné la dépendance la RPDC à l'égard des réseaux criminels organisés ou transnationaux, exploitant leurs couloirs de transport et leurs intermédiaires pour soutenir les activités de prolifération.

Vulnérabilités sectorielles en matière de PF et d'évasion des sanctions

48. D'après les contributions du Réseau mondial du GAFI et les résultats de la consultation publique, les secteurs les plus vulnérables aux systèmes complexes de financement du terrorisme et d'évasion des sanctions comprennent :

Secteur bancaire et autres secteurs financiers

49. De nombreux pays ont identifié le secteur bancaire et d'autres secteurs financiers, comme celui des assurances, comme vulnérables aux menaces de fraude fiscale et de contournement des sanctions. Une fois les transactions financières terminées,

Menés à l'intérieur des pays et au-delà des frontières, les fonds soutenant les acteurs ou les activités du PF peuvent être générés ou transiter par des activités licites ou illicites. Les techniques souvent utilisées pour

brouiller la nature de ces transactions implique l'utilisation de plusieurs comptes et documents falsifiés, notamment liés au financement du commerce.

50. Les banques correspondantes sont vulnérables au contournement des sanctions car elles n'ont souvent pas de relation préexistante avec le client de la banque concernée. 30 Plusieurs entités du secteur privé ont identifié divers types de comptes et de transactions complexes vulnérables au risque de PF et de contournement des sanctions, ce qui est particulièrement pertinent pour les relations de banque correspondante impliquant des liens avec des pays présentant une exposition plus élevée au risque de PF et/ou des contrôles CPF inefficaces. Par exemple, les transactions effectuées via des transactions à compte ouvert sont vulnérables, car elles manquent d'informations sur les marchandises transportées. De plus, les virements électroniques permettent des mouvements de fonds rapides, mais ils contiennent généralement peu d'informations sur l'objet de la transaction ou les pièces justificatives.

51. Certains pays ont identifié plusieurs autres facteurs pertinents, notamment des systèmes financiers dotés de vastes réseaux nationaux, un accès rapide et facile aux services bancaires, une augmentation du montant des actifs d'investissement en circulation et une abondance d'actifs financiers détenus par les particuliers.

Actifs virtuels et fournisseurs de services d'actifs virtuels

52. De nombreux pays s'inquiètent de l'utilisation croissante d'actifs virtuels pour effectuer des paiements et des transferts transfrontaliers. Les réseaux de FP cherchent souvent à exploiter l'absence de mise en œuvre effective des mesures de LBC/FT/CPF pour les PSAV dans différents pays, compte tenu du retard dans la mise en œuvre de la Recommandation 15 (voir Typologie 3). On observe également des cas de PSAV dans des pays appliquant des exigences en matière de LBC/FT/CPF qui ne respectent pas les obligations applicables. Les pays sont particulièrement préoccupés par les risques associés aux FP liés à la collecte et au transfert de fonds sous pseudonyme. De nombreux acteurs illicites cherchent à accroître l'anonymat lors des transactions d'actifs virtuels en utilisant des services de mixage d'actifs virtuels et des cryptomonnaies améliorant l'anonymat (AEC), notamment dans le cadre du blanchiment des produits de vols d'actifs virtuels à grande échelle qui favorisent la prolifération des armes de destruction massive. Le recours au mixage et à d'autres techniques d'obscurcissement peut rendre difficile pour des tiers le traçage ou l'attribution des transactions. Par ailleurs, les pays ont souligné le rôle des actifs virtuels dans les activités de génération de revenus de la RPDC.

Infrastructures de paiement nouvelles et alternatives

53. Certains acteurs étatiques et non étatiques explorent de nouveaux canaux de paiement et des alternatives au système SWIFT afin d'éviter les points de contact financiers liés aux régimes de sanctions nationaux, supranationaux et/ou internationaux. Par exemple, dans certains cas, les acteurs étatiques et non étatiques pourraient utiliser des systèmes de paiement numérique émergents, tels que les services de paiement peer-to-peer ou les prestataires de transfert de fonds numériques. 31

30 Les services de correspondance bancaire, en particulier ceux proposés à des juridictions connues pour leur capacité de détournement ou de transfert, ou dont les contrôles de LBC/FT/CPF sont inefficaces, peuvent présenter des risques accrus. Cependant, le risque de correspondance bancaire n'est pas uniformément élevé en matière de financement de la prolifération. L'évaluation des risques liés aux relations de correspondance bancaire doit être effectuée au cas par cas et doit toujours tenir compte des contrôles internes et des mesures d'atténuation des risques appliqués par la banque concernée. Pour plus d'informations sur les relations de correspondance bancaire, consultez les lignes directrices 2021 du GAFI sur les relations de correspondance bancaire.

31 Bien que les alternatives au système de messagerie de paiement SWIFT suscitent des inquiétudes en matière de gestion des risques, l'utilisation des monnaies numériques de banque centrale (MNBC) pour échapper aux sanctions est pour l'instant théorique. D'autre part, certains pays considèrent les MNBC comme un moyen pour les autorités compétentes de suivre plus facilement les flux de fonds et de réduire les risques financiers illicites.

Autres vulnérabilités au niveau sectoriel

54. Comme indiqué dans les rapports POE de la résolution 1718 du Conseil de sécurité des Nations Unies et dans les Orientations 2021 du GAFI sur l'évaluation et l'atténuation des risques liés aux PF, les pays doivent être conscients des secteurs supplémentaires plus exposés à la violation, à la non-mise en œuvre ou à l'évasion potentielles des PF-TFS, y compris, mais sans s'y limiter : les prestataires de services aux fiducies et aux sociétés (TSPS) et les négociants en métaux précieux et en pierres précieuses.32

55. En outre, les pays ont identifié plusieurs autres secteurs vulnérables à l'exploitation des PF et des acteurs de l'évasion des sanctions, notamment l'aéronautique, les technologies de l'information (TI), le transport maritime, l'énergie nucléaire et la construction navale.

32. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk- Assessment-Mitigation.pdf

4. Section 2. Évasion des sanctions relatives au PF – Typologies

Tendances et méthodes actuelles

56. Dans ce rapport, les études de cas sont séparées en deux catégories distinctes :

a. Évasion des PF-TFS liés à la RPDC, qui est couverte par la recommandation 7 des normes du GAFI
b. Évasion d'autres régimes de sanctions (tels que les sanctions nationales et supranationales), qui ne sont pas couverts par la recommandation 7 des normes du GAFI

57. Cette section vise à fournir une liste non exhaustive des typologies utilisées dans les schémas complexes de fraude fiscale et d'évasion des sanctions, sur la base des informations fournies par le Réseau mondial du GAFI. Ces typologies ont permis d'établir une liste d'indicateurs de transactions financières susceptibles d'être révélateurs de fraude fiscale (voir Annexe A : Indicateurs de risque).

Tableau 1. Aperçu des typologies

Typologie	Sous-thèmes des études de cas	Pages
1. Recrutement d'intermédiaires pour échapper aux sanctions	Sociétés écrans et sociétés écrans Transit par des pays tiers Comptes bancaires et financement	25-33
2. Obscurcir l'accès au système financier par le BOI	Facilitateurs tiers soutenant l'accès financier Réseaux de facilitateurs financiers non agréés Utilisation de différents types de personnes morales Exploitation des cartes de crédit et de débit par la RPDC	33-40
3. Utilisation d'actifs virtuels et d'autres technologies	Défis réglementaires Utilisation d'actifs virtuels pour déplacer des fonds Actifs virtuels et génération de fonds Entités et individus étrangers soutenant les technologies de l'information de la RPDC Ouvriers	40-47
4. Exploiter les secteurs maritime et maritime	Modification de l'identifiant du navire Transferts de navire à navire Désactivation de la diffusion AIS Falsification de documents	47-52

Typologie 1 : Recrutement d'intermédiaires pour échapper aux sanctions

58. Les pays signalent que pour dissimuler les véritables utilisateurs finaux, les réseaux d'approvisionnement en biens destinés aux pays proliférants ou sanctionnés recourent à des stratagèmes complexes impliquant plusieurs intermédiaires. Ces tactiques compliquent la détection et les enquêtes sur les cas de fraude financière et de contournement des sanctions. Ces intermédiaires peuvent impliquer des sociétés écrans et de façade, des facilitateurs financiers, des comptes bancaires (y compris des relations de correspondant bancaire) et des transbordements via des pays tiers. Le recours à ces intermédiaires joue un rôle crucial dans le masquage de l'origine, de la destination et de l'objet des fonds. En exploitant les vulnérabilités des différents systèmes financiers et cadres réglementaires, les intermédiaires favorisent la prolifération.

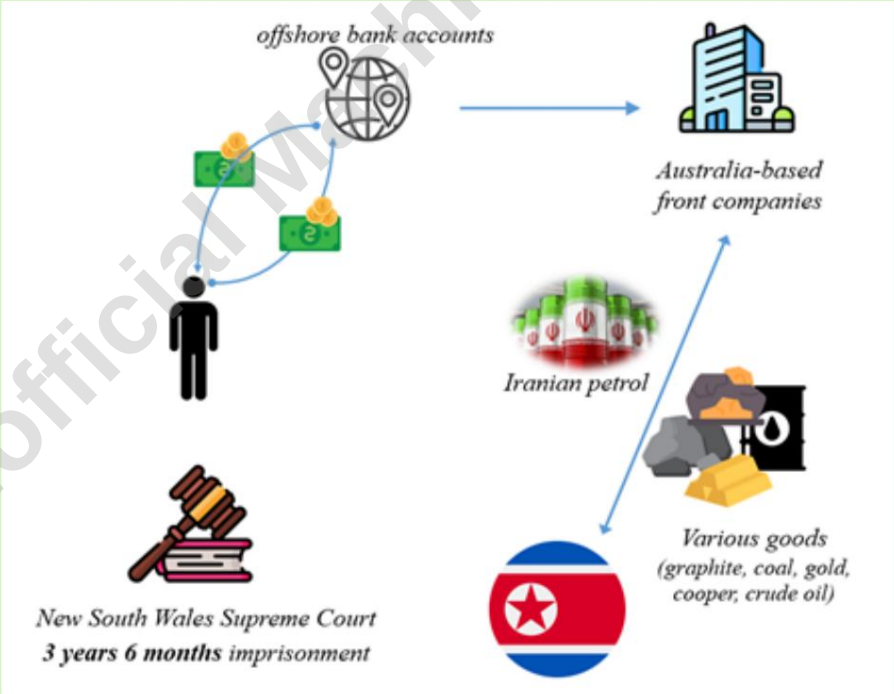
réseaux pour échapper à la détection et aux sanctions (voir la section Vulnérabilités pour plus d'informations).

Utilisation de sociétés écrans et de sociétés-écrans

59. De nombreux pays ont signalé que les réseaux de financement du terrorisme et de contournement des sanctions peuvent créer des entreprises locales dans des pays tiers ou s'associer à elles pour servir d'intermédiaires et de sociétés écrans. Ces entités peuvent être des sociétés écrans sans activité ou effectuer des transactions apparemment légitimes pour accéder aux systèmes financiers, faciliter les paiements et les contrats, importer ou exporter des marchandises sous de faux prétextes (par exemple, en déclarant des biens à double usage comme étant exclusivement destinés à des fins civiles) et masquer leurs liens avec les entités sanctionnées en opérant sous des noms, des structures de propriété ou des pays différents. Les acteurs illicites opèrent dans des secteurs liés aux biens ou articles à double usage de contrebande, tels que l'électronique, les produits chimiques ou les équipements industriels, ou d'autres biens soumis à des sanctions ou à des réglementations de contrôle des exportations.

Encadré 2. Étude de cas : Utilisation d'une structure d'entreprise basée en Australie pour échapper aux sanctions

Le 23 juillet 2021, la Cour suprême de Nouvelle-Galles du Sud a condamné un citoyen australien né en Corée du Sud à une peine de trois ans et six mois d'emprisonnement pour avoir enfreint la loi australienne sur les sanctions contre la RPDC. L'individu a utilisé des comptes bancaires offshore et une série de sociétés écrans basées en Australie pour négocier avec la RPDC des échanges commerciaux portant sur divers produits, notamment du charbon, du graphite, du minerai de cuivre, de l'or, du pétrole brut (y compris l'achat d'essence iranienne pour le compte de la RPDC), des missiles et des technologies liées aux missiles. C'était la première fois que des accusations étaient portées en Australie pour violation des sanctions contre la RPDC.



Source : Australie

60. Les intermédiaires peuvent également faire appel au soutien d'avocats et de comptables qui aident à mettre en place des structures complexes pour éviter d'être détectés, ou de transitaires et d'agents maritimes qui aident à créer des chaînes d'approvisionnement complexes et fournissent des conseils sur la manière d'exploiter les failles des régimes de sanctions et de garantir que les marchandises interdites sont mal déclarées et expédiées sous de faux prétextes.

Les sociétés écrans constituent un moyen courant de dissimuler la destination finale des biens à double usage, notamment dans le secteur de l'armement militaire ou de la défense. Les acteurs illicites utilisent ces types de mécanismes complexes pour ralentir les enquêtes visant à révéler les cas potentiels d'évasion de sanctions ou de contournement des contrôles à l'exportation de biens sensibles. Les deux études de cas ci-dessous décrivent des stratagèmes complexes visant à dissimuler la destination finale de ces biens à double usage.

Encadré 3. Étude de cas : Projet d'évasion des sanctions visant à introduire en contrebande des composants électroniques d'origine américaine vers des entités militaires iraniennes

En janvier 2024, quatre ressortissants chinois ont été inculpés dans le district de Columbia de divers crimes fédéraux liés à un complot de plusieurs années visant à exporter illégalement et à faire passer en contrebande des composants électroniques d'origine américaine des États-Unis vers l'Iran. Les accusés auraient exporté illégalement et fait passer en contrebande des articles américains contrôlés à l'exportation via la Chine et Hong Kong au profit d'entités affiliées au Corps des gardiens de la révolution islamique (CGRI) et au ministère de la Défense et de la Logistique des forces armées (MODAFL), qui supervisent le développement et la production iraniens de missiles, d'armes et d'équipements aériens militaires, notamment de drones.

Dès mai 2007 et jusqu'en juillet 2020 au moins, les individus a utilisé des sociétés écrans en Chine pour acheminer des articles à double usage d'origine américaine, notamment des produits électroniques et des composants qui pourraient être utilisés dans la production de drones, de systèmes de missiles balistiques et d'autres utilisations militaires finales, vers des entités sanctionnées ayant des liens avec le CGRI et le MODAFL, telles que Shiraz Electronics Industries (SEI), Rayan Roshd Afzar et leurs filiales.

Tout au long du complot, les accusés ont dissimulé la destination des marchandises en Iran et à des entités iraniennes, et ont fourni de fausses déclarations aux entreprises américaines concernant leur destination finale et leurs utilisateurs finaux. Ces pratiques trompeuses ont incité les entreprises américaines à exporter des biens à double usage vers des sociétés écrans sous de faux prétextes, prétendant que la destination finale de ces produits était la Chine et non l'Iran, en violation des lois et réglementations américaines sur les sanctions et le contrôle des exportations. Les accusations liées à ce complexe stratagème de contournement des sanctions ont été coordonnées par une force de frappe interinstitutionnelle codirigée par les ministères de la Justice et du Commerce.

Source : États-Unis

Encadré 4. Étude de cas : Exportation de biens à double usage vers une entité russe en utilisant des intermédiaires

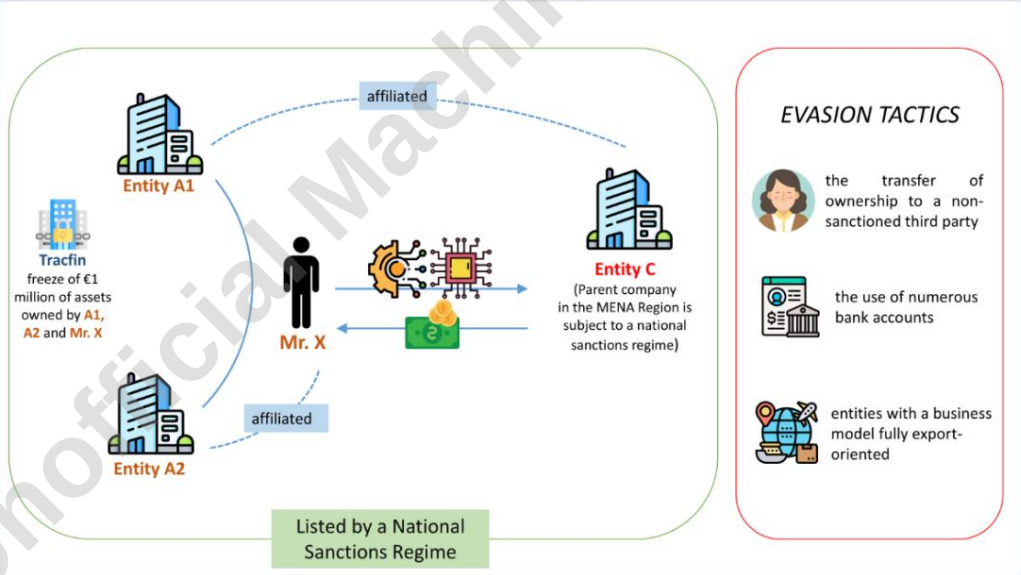
Les sociétés françaises A1 et A2 ont agi comme intermédiaires pour l'achat de composants électroniques étrangers, revendus à une autre entité intermédiaire de la région MENA (Entité B). Après l'achat des biens à double usage, les intermédiaires ont fourni les composants électroniques à une société mère russe sanctionnée par les États-Unis (Entité C).

Ce programme proliférant a permis au secteur de la défense russe de s'approvisionner en articles interdits et d'améliorer ses capacités globales.

La cellule de renseignements financiers française, TracFin, a mené une action interinstitutionnelle pour mettre fin à ce stratagème en gelant 1 million d'euros d'actifs appartenant à A1, A2 et M. X (UBO de A1 et A2). Alors que les États-Unis L'OFAC du Trésor a sanctionné A1, A2 et M. X. Ces personnes et entités ne sont pas soumises aux mesures restrictives de l'UE ou de la France pour le moment. Par la suite, TracFin a collaboré avec les banques françaises pour restreindre leurs fonds conformément aux critères de contrôle33, car il était suspecté que l'entité C détienne toujours le contrôle de la société A1 malgré la vente de ses actions à un investisseur étranger. L'entité A2 est détenue à 100 % par M. X.

Ce système complexe d'évasion des sanctions impliquait l'utilisation de nombreuses tactiques d'évasion courantes, notamment le transfert de propriété à un tiers non sanctionné (l'épouse de l'individu), l'utilisation de nombreux comptes bancaires et d'entités ayant un modèle économique entièrement orienté vers l'exportation, qui agissaient néanmoins comme des entités de passage.

Le principal défi était la divergence entre les régimes de sanctions, [34] qui pourrait entraîner une fuite des capitaux. Des processus de désignation concertés seraient bénéfiques pour garantir l'efficacité des sanctions et garantir l'existence d'une base juridique pour le gel des avoirs dans tous les pays.



Source : France

Utilisation du transit dans les pays tiers pour tirer parti des chaînes d'approvisionnement mondialisées et Commerce international

62. Les pays ont décrit des réseaux de prolifération utilisant des chaînes d'approvisionnement mondialisées et le commerce international pour occulter les activités d'approvisionnement en biens et en technologies. Ils peuvent

Ils s'approvisionnent en composants auprès de multiples fournisseurs afin de masquer la nature de l'utilisation finale et transfèrent les marchandises via des zones franches (ZF), souvent moins surveillées et autorisant le reconditionnement et la réexportation sous de nouvelles étiquettes. Les marchandises peuvent transiter par plusieurs ports ou pays afin de masquer leur véritable origine ou destination, en utilisant de faux documents, des documents d'expédition falsifiés, des certificats d'utilisateur final ou des connaissements, afin de dénaturer la nature de la cargaison ou le destinataire final. Par exemple, une cargaison interdite de composants de missiles peut être déguisée en machines industrielles avec des documents falsifiés. Les deux études de cas ci-dessous décrivent des itinéraires de transit complexes afin de rendre plus difficile la détection du contournement des réglementations et des sanctions en matière de contrôle des exportations.

Encadré 5. Étude de cas : Utilisation d'intermédiaires pour contourner les réglementations en matière de contrôle des exportations

Plusieurs cas, tendant à illustrer une typologie récurrente, mettent en évidence des schémas de contournement où des entreprises de pays tiers, parfois basées dans une autre juridiction de l'UE, gérées ou contrôlées par des Iraniens, achètent des biens à double usage auprès de fournisseurs français, qui sont ensuite réexportés vers l'Iran.

Une entreprise iranienne fournissant le programme de missiles balistiques iranien a tenté d'obtenir des matériaux composites auprès d'un fournisseur français. Le dirigeant iranien de l'entreprise a fait appel à une société d'un pays tiers dirigée par un autre ressortissant iranien, qui réexportait ensuite les matériaux composites vers l'Iran.

En 2020, une machine-outil a été exportée successivement vers les pays européens A, B et C avant de quitter le territoire de l'UE. Ce schéma commercial complexe et les modifications apportées à la documentation visaient à dissimuler la suite du voyage, qui incluait l'arrivée dans une juridiction du Moyen-Orient avant que la machine-outil n'atteigne sa destination finale en Iran.

Source : France

Encadré 6. Étude de cas : Détection du contournement des sanctions de l'UE par le recours à des intermédiaires dans le cadre de la coopération internationale

En 2022, une entreprise portugaise a tenté d'exporter des moteurs destinés à des drones via un intermédiaire aux Émirats arabes unis, avec une prétendue destination finale vers une entreprise basée au Kazakhstan. Ces marchandises étaient couvertes par le 12e paquet de mesures restrictives de l'UE à l'encontre de la Russie, et tout portait à croire que la destination finale des marchandises serait la Fédération de Russie. Au cours de l'enquête, l'entreprise a abandonné l'exportation des marchandises après que des questions ont été soulevées quant à leur destination.

L'entreprise a tenté de contourner les sanctions en utilisant deux intermédiaires : un transitaire aux Émirats arabes unis et un détaillant au Kazakhstan. Elle a également dissimulé la finalité de l'opération. utilisateur. La société kazakhe entretenait des liens commerciaux étroits avec des entreprises russes et

En droit européen , les critères de contrôle permettent de déterminer si des fonds ou une entité sont contrôlés par une entité ou une personne sanctionnée. Par exemple, si la personne ou l'entité sanctionnée exerce une influence ou peut prendre des décisions sur les fonds ou l'entité, cela peut aider à déterminer l'existence d'un contrôle.

34 Cette divergence est l'un des facteurs clés des difficultés rencontrées pour détecter, enquêter et poursuivre les cas de contournement des sanctions concernant le PF, comme indiqué dans la section 3 (voir paragraphes 105-106) et en conclusion (voir paragraphe 146 et domaines prioritaires).

Le risque de détournement était élevé. Les paiements étaient effectués par virement bancaire.

Par la suite, les autorités portugaises ont surveillé l'entreprise et découvert qu'elle avait exporté, plus tard en 2023, d'autres biens dans le domaine de la sécurité et de la défense, probablement vers la Russie, par l'intermédiaire d'intermédiaires en Serbie et à Hong Kong. Ces deux intermédiaires entretenaient des relations commerciales étroites avec la Fédération de Russie.

L'affaire a nécessité la coopération du Service de renseignement de sécurité et de l'Autorité douanière. Elle a été découverte grâce à la collecte de renseignements et a fait l'objet d'une enquête grâce à la coopération internationale et aux enquêtes douanières.

Cet exemple illustre la capacité des réseaux d'approvisionnement à s'adapter aux nouvelles circonstances et aux différents défis. Seule une coopération efficace entre les pays est nécessaire.
Une communication fluide peut aider à atténuer ce type de menace.

Source : Portugal

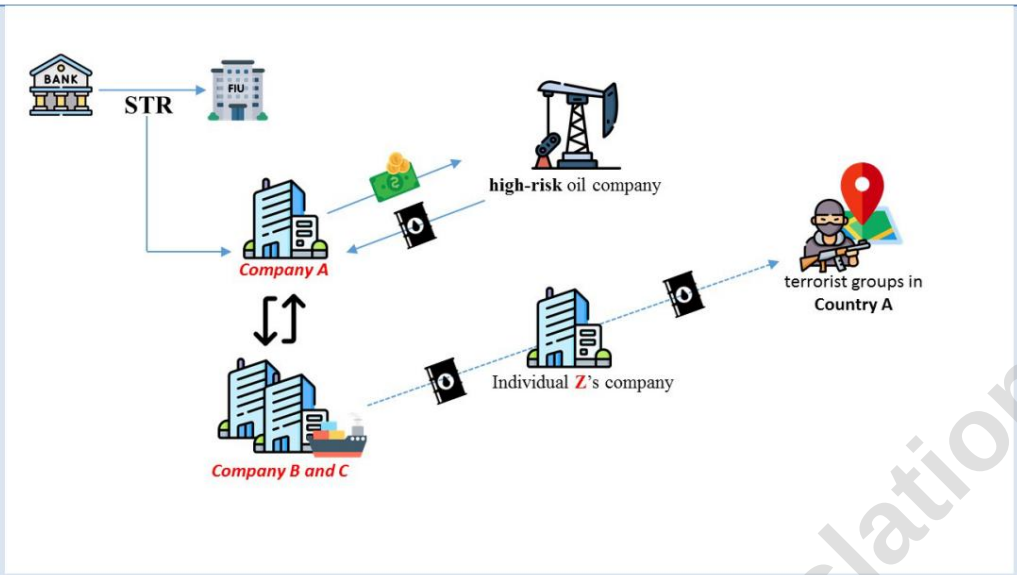
63. De plus, les plateformes de transit régionales proches des pays ou entités sanctionnés sont la cible de fraudeurs cherchant à transférer des fonds et des marchandises. Le PF et les réseaux de sanctions cherchent notamment à dissimuler leurs activités dans les centres financiers internationaux, où ils espèrent que l'ampleur des activités commerciales et financières contribuera à masquer leurs activités illicites.

Encadré 7. Étude de cas : Utilisation de compagnies maritimes pour vendre du pétrole au nom d'une entité sanctionnée

En septembre 2022, les LEA ont reçu une diffusion de l'UAEFIU concernant un SAR/STR d'une banque. Le SAR/STR a mis en évidence un virement bancaire de la société A à une compagnie pétrolière à haut risque, soupçonnée d'être utilisée pour soutenir la prolifération des armes de destruction massive. Les services répressifs et l'UAEFIU ont mené une enquête criminelle et financière sur la société A et ses activités financières et commerciales.

L'enquête a révélé que la société A avait été créée par un ressortissant étranger, lié à deux compagnies maritimes des Émirats arabes unis (sociétés B et C). Elle a également révélé que les sociétés B et C appartenaient à des individus soutenant des groupes terroristes dans le pays A.
Les deux sociétés ont utilisé la société de l'individu Z comme intermédiaire pour préparer des contrats d'expédition pour le transport du pétrole du pays à haut risque vers les sociétés B et C, qui devaient ensuite être expédiés au groupe terroriste.

L'enquête a également révélé que les sociétés B et C vendaient du pétrole au groupe terroriste en utilisant de faux documents pour dissimuler la source et l'origine du pétrole. Le produit de ces ventes était transféré à la société A, qui le transmettait à la compagnie pétrolière à haut risque – une façade présumée utilisée par l'entité sanctionnée pour soutenir la prolifération. L'enquête a permis d'établir que le montant total des fonds transférés s'élevait à 70 millions de dollars américains. Les forces de l'ordre ont arrêté tous les suspects, y compris l'individu Z, qui a avoué son implication dans l'aide apportée à l'Iran pour contourner les sanctions du Front Polisario, et ont suspendu les activités commerciales des sociétés.



Source : Émirats arabes unis

Utilisation de comptes bancaires et financement par l'intermédiaire de pays tiers

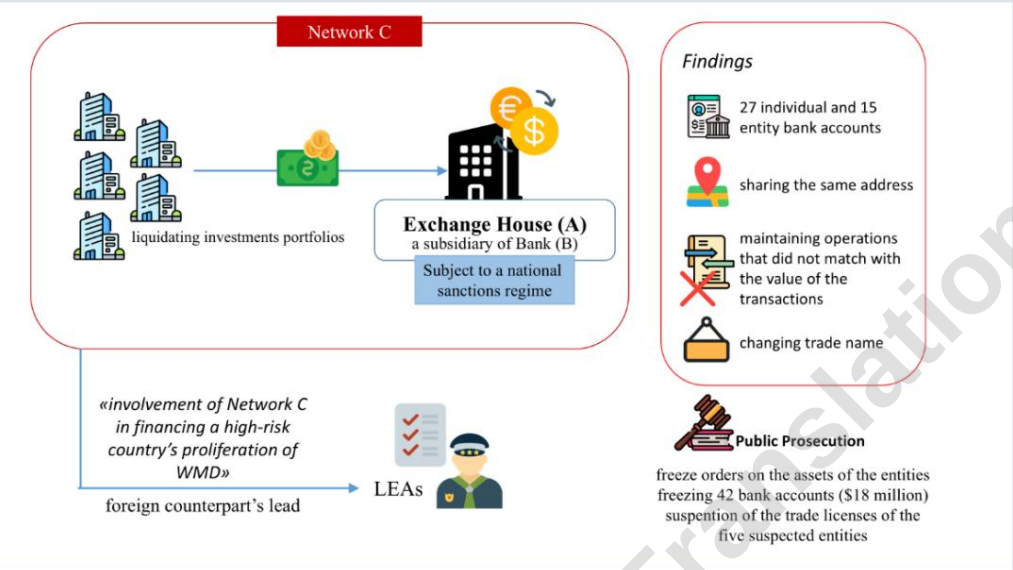
64. Les acteurs du blanchiment d'argent et de l'évasion des sanctions recourent souvent à de multiples strates de transactions financières pour dissimuler l'origine, la destination ou l'objet des fonds, une technique classique de blanchiment d'argent. Ils acheminent souvent les paiements par l'intermédiaire de multiples institutions financières réparties dans plusieurs pays afin d'entraver les efforts de traçage, avec des sociétés écrans enregistrées dans des pays présentant des failles réglementaires.

Encadré 8. Étude de cas : Utilisation abusive du système financier et des expéditions de pétrole pour soutenir le PF

Les services répressifs ont identifié, grâce à des sources confidentielles, de multiples transactions entrantes et sortantes de grande valeur effectuées par cinq sociétés émiraties avec la maison de change à haut risque (A), filiale de la banque (B). La maison de change A et la banque B font toutes deux partie du « Réseau C » et sont désignées par l'OFAC du Trésor américain. Deux des cinq sociétés suspectées obtenaient des fonds en liquidant des portefeuilles d'investissement et en les transférant à la maison de change A, qui les transférait à son tour à la banque B pour soutenir une entité sanctionnée. Les services répressifs ont ouvert une enquête auprès des parties prenantes concernées (UAEFIU, CBUAE, bureaux d'enregistrement locaux et douanes).

La CBUAE a identifié 27 comptes bancaires individuels et 15 comptes bancaires d'entités liés au réseau. Les registres locaux ont également fourni aux services répressifs des rapports d'inspection sur place ; ces rapports ont révélé que les entités suspectées partageaient la même adresse, avaient tendance à changer de raison sociale avant la visite sur place et exerçaient des activités qui ne correspondaient pas au montant des transactions. Parallèlement, les services répressifs ont reçu une piste d'un homologue étranger confirmant l'implication du Réseau C dans le financement de la prolifération d'armes de destruction massive dans un pays à haut risque.

Sur la base de ces conclusions, le ministère public, en coordination avec l'UAEFIU et la CBUAE, a émis des ordonnances de gel des actifs des entités, gelant 42 comptes bancaires pour un solde total d'environ 18 millions de dollars (63 725 065 AED). De plus, les greffiers locaux ont suspendu les licences commerciales des cinq entités suspectées.



Source : Émirats arabes unis

65. Les réseaux de PF ciblent les institutions financières de pays tiers où ils cherchent à exploiter les différences juridictionnelles dans la mise en œuvre des régimes de sanctions internationaux et nationaux. Les acteurs illicites utilisent les banques pour ouvrir des comptes et faciliter les virements internationaux sans déclencher d'alerte, en utilisant des relations de correspondant bancaire pour accéder indirectement aux marchés financiers internationaux. Les réseaux illicites peuvent également utiliser des systèmes financiers informels, moins susceptibles de détecter les transactions suspectes.
s'appuyer sur des pays ayant des exigences de déclaration ou d'application moins strictes pour les transactions transfrontalières.

Encadré 9. Étude de cas : Entités et individus sanctionnés pour avoir constitué un réseau bancaire parallèle utilisé par le CGRI pour générer des revenus

En juin 2024, l'OFAC a sanctionné près de 50 entités et individus qui constituent de multiples branches d'un vaste réseau de « banque parallèle » utilisé par le MODAFL et le CGRI pour générer des revenus afin, entre autres activités, d'obtenir illégalement les États-Unis.
composants électroniques d'origine pour développer des armes avancées, telles que des drones, et soutenir les Houthis du Yémen et la guerre de la Russie en Ukraine.

Pour accéder au système financier international, le MODAFL utilise des bureaux de change en Iran qui gèrent de nombreuses sociétés écrans à Hong Kong, aux Émirats arabes unis et ailleurs afin de blanchir les revenus générés par ses activités commerciales à l'étranger, notamment les ventes de pétrole, en devises étrangères propres. Ces mêmes sociétés écrans utilisent ces devises blanchies pour se procurer des composants d'armes sur le marché international.

Source : États-Unis

Encadré 10. Étude de cas : Utilisation d'intermédiaires pour contourner le TFS et transférer les revenus générés par l'immobilier

En 2015, un diplomate de la RPDC en poste en France a acheté un appartement à Paris et l'a loué, avant d'être désigné par l'ONU en 2017. Après avoir été sanctionné, il a continué à percevoir les revenus générés par la location de l'appartement. L'individu a mis au point un système impliquant divers intermédiaires disposant de comptes bancaires dans plusieurs pays tiers, dissimulant ainsi son statut de bénéficiaire final. Après l'alerte lancée par une banque européenne en 2019, les revenus ont été placés sur un compte séquestre.

Source : France

Typologie 2 : Obscurcir le BOI pour échapper aux sanctions et accéder au système financier

66. Les fraudes complexes aux sanctions et aux PF impliquent souvent la falsification des BOI, obscurcissant ainsi l'utilisateur final, l'utilisation finale et la destination finale, ce qui est difficile à détecter, tant pour le secteur public que privé. De plus, nombre de ces techniques d'obscurcissement sont appliquées au monde numérique, ce qui peut compliquer encore la détection. Étant donné que les TFS s'appliquent aux personnes et entités désignées, ainsi qu'aux fonds contrôlés ou détenus par ces personnes, l'identification des bénéficiaires effectifs peut contribuer à atténuer les risques liés au contournement des sanctions.

Facilitateurs tiers soutenant l'accès de la RPDC au système financier

67. La RPDC recourt régulièrement à des pratiques trompeuses, notamment en masquant les informations sur les banques d'investissement (BOI), pour contourner les régimes de sanctions de l'ONU et des États-Unis et accéder au système financier officiel. Elle continue de recourir à des sociétés écrans et à des sociétés écrans basées à l'étranger, à des représentants clandestins à l'étranger et à des intermédiaires tiers pour dissimuler l'identité du véritable émetteur, du bénéficiaire et de l'émetteur.

et le but des transactions, permettant à des milliards de dollars d'activités financières illicites de la RPDC de circuler à travers le système financier international. Les acteurs étatiques qui soutiennent les stratagèmes complexes de la RPDC pour accéder au système financier rendent difficile la lutte contre l'évasion des sanctions.

Encadré 11. Étude de cas : La RPDC et des entités financières russes ont orchestré un système complexe d'évasion des sanctions

En septembre 2024, l'OFAC du Trésor américain a désigné un réseau de cinq entités et un individu – basés en Russie et dans la région géorgienne d'Ossétie du Sud occupée par la Russie – qui utilisaient des stratagèmes financiers illicites pour permettre à la RPDC d'accéder au système financier international en violation du TFS requis par la résolution 1718 du Conseil de sécurité des Nations unies.35

En outre, les entités et les individus ont violé l'interdiction des relations de correspondance avec les banques de la RPDC en vertu de la résolution 2270 du Conseil de sécurité des Nations Unies.

Français Cette action visait des stratagèmes complexes orchestrés par deux organisations étatiques de la RPDC, la Foreign Trade Bank (FTB) et la Korea Kwangson Banking Corporation (KKBC), toutes deux désignées comme entités sur la liste des sanctions de la résolution 1718 du Conseil de sécurité des Nations Unies.36 La FTB est la principale banque de change de devises de la RPDC et est essentielle aux réseaux financiers illicites que la RPDC utilise pour financer ses programmes d'armes de destruction massive et de missiles balistiques. La FTB et la KKBC ont continué d'élargir l'accès de la RPDC aux réseaux financiers illicites avec l'aide de la Fédération de Russie.

Dans le cadre d'un stratagème orchestré par la Banque centrale de Russie, la banque MRB (MRB), basée en Ossétie du Sud en Géorgie, a servi d'intermédiaire à une banque russe, la TSMR Bank, OOO (TSMR Bank), afin d'établir une relation bancaire secrète avec la FTB. Un haut responsable de la TSMR Bank a facilité les dépôts d'espèces de la FTB via la TSMR Bank à la MRB. Ce haut responsable a organisé l'ouverture de comptes correspondants pour la FTB et la KKBC à la MRB et a coordonné avec les représentants de la RPDC la livraison de millions de dollars et de roubles en billets de banque sur les comptes de la FTB et de la KKBC à la MRB. Au moins certains des comptes de la RPDC à la MRB ont été utilisés pour payer les exportations de carburant de la Russie vers la RPDC.

Dans le cadre d'un plan distinct, fin 2023, la Russian Financial Corporation Bank JSC (RFC) a collaboré avec FTB pour créer une société basée à Moscou, Stroytreyd LLC (Stroytreyd), afin de recevoir les fonds gelés de la RPDC détenus dans des banques russes en faillite. Dans le cadre de cet effort de rapatriement des avoirs gelés en RPDC, Timer Bank, AO (Timer Bank), propriété de RFC, a transféré des fonds d'une valeur de plusieurs millions de dollars à Stroytreyd, au bénéfice ultime de FTB. Les responsables du gouvernement de la RPDC ont collaboré avec la RFC pour accroître les échanges économiques de haut niveau entre la RPDC et la Russie et pour renforcer la collaboration financière entre les deux pays. FTB a également collaboré avec RFC pour ouvrir des comptes pour d'autres banques de la RPDC, notamment la Banque de développement agricole basée en RPDC.
37

Source : États-Unis

35 https://home.treasury.gov/news/press-releases/jy2590 36 Sur la liste de la résolution 1718 du Conseil de sécurité des Nations Unies, FTB est désigné comme KPe.047 et KKBC comme KPe.025. 37 Le 10 janvier 2025, le Japon a désigné quatre personnes et cinq entités (MRB Bank, Russian Financial Cooperation, Stroytreyd LLC, TsMRBank et Timer Bank AO) pour faciliter la coopération entre la RPDC et la Russie.

68. Comme l'ont indiqué de nombreux pays, la RPDC compte également sur ses citoyens, y compris son personnel diplomatique, pour faciliter la fourniture de services financiers ou le transfert d'actifs ou de ressources, notamment le transport d'espèces. Ces tactiques sont difficiles à détecter, et les protocoles diplomatiques rendent encore plus difficile l'intervention rapide pour intercepter ou perturber ces activités.

Encadré 12. Étude de cas : L'épouse d'un diplomate de la RPDC transfère des fonds par l'intermédiaire d'une compagnie d'assurance

Des compagnies d'assurance basées au Nigéria étaient soupçonnées de collaborer avec l'épouse d'un diplomate d'un pays sanctionné pour aider la compagnie d'assurance nationale de la RPDC, la Korea National Insurance Company (KNIC), à recouvrer des créances, à développer ses activités, à collecter des fonds, à effectuer des transferts financiers et à agir en tant qu'agents ou représentants pour contourner les sanctions des Nations Unies. La KNIC a été désignée comme telle en 2017 au titre du régime de sanctions de la résolution 1718 du Conseil de sécurité des Nations Unies (KPe.048). L'argent reçu par l'intermédiaire de la KNIC est détourné vers les programmes d'armes de destruction massive de la RPDC.

Un signalement d'activité suspecte (SAR/DOS) déposé par une institution financière a permis aux autorités nigérianes de détecter des activités financières impliquant des montants excessifs. Le montant total des transactions estimatif dépassait 616 000 €. Suite à l'identification de l'activité suspecte, les institutions financières ont gelé les comptes concernés et signalé ces activités aux autorités nigérianes. Le Nigéria envisage également de nouvelles mesures de lutte.

La vulnérabilité ciblée dans le secteur des assurances résidait dans la manière dont les compagnies d'assurance souscrivent des assurances ou des réassurances internationales pour les infrastructures publiques par l'intermédiaire de sociétés tierces. De plus, les clients et les transactions des compagnies d'assurance étaient utilisés pour échapper aux sanctions, ce qui démontre la nécessité de renforcer les contrôles des risques pour les entités concernées.

Source : Nigéria

69. De nombreux pays savent que la RPDC utilise des ressortissants étrangers et des sociétés écrans enregistrées par ces mêmes personnes pour tromper la BOI et lui permettre d'accéder au système financier officiel et de transférer des fonds. Par exemple, FTB et KKBC ont occulté leurs liens financiers avec la RPDC en créant des réseaux de sociétés écrans au nom de ressortissants chinois.
détenir des comptes dans des banques basées en Chine, pour transférer des fonds à travers le système financier international.

Encadré 13. Étude de cas : Services bancaires et financiers de la RPDC – Banque du commerce extérieur

En mai 2020, les autorités américaines ont rendu publiques les accusations criminelles portées contre plus de 30 personnes ayant prétendument fourni des services et effectué des transactions interdites en dollars américains pour le compte de FTB désignés par l'ONU. L'acte d'accusation détaillait des paiements spécifiques effectués à des entreprises américaines pour le compte du gouvernement de la RPDC. D'autres paiements entre des sociétés écrans de FTB et des sociétés tierces ont été compensés par des banques correspondantes américaines.

Les individus mentionnés dans l'acte d'accusation ont fait traiter par des banques correspondantes au moins 2,5 milliards de dollars de paiements illégaux, via plus de 250 sociétés écrans, transitant par les États-Unis pendant la période du complot. Ces sociétés étaient établies en Autriche, en Chine, au Koweït, en Libye, aux Îles Marshall, en Russie et en Thaïlande. Nombre des individus inculpés étaient en poste dans ces pays, gérant des « antennes » secrètes de la FTB, dont de nombreuses activités importantes étaient concentrées dans des villes chinoises.

Les individus ont collaboré avec des intermédiaires financiers tiers pour créer des sociétés écrans capables d'effectuer des paiements pour l'achat de matières premières et d'autres biens au nom de la RPDC, notamment des paiements liés au commerce de pétrole raffiné et de charbon. D'autres paiements ont été effectués à des entreprises des secteurs des métaux, de l'électronique et des télécommunications. Les accusés ont créé de nouvelles sociétés écrans lorsque leurs contreparties ont jugé les anciennes suspectes. Ils ont utilisé des références de paiement codées dans les communications entre les agents de la FTB afin que le siège de la FTB puisse orienter les achats et conserver une évaluation précise des flux de fonds de leurs sociétés écrans vers les bénéficiaires. Enfin, concernant l'expédition des marchandises, les accusés ont étiqueté les contrats et les factures avec de fausses destinations finales et des termes de transaction erronés.

utilisateurs.

Source : États-Unis

Des réseaux de facilitateurs financiers non agréés favorisent l'évasion des sanctions

70. Par ailleurs, plusieurs pays ont identifié le recours par l'Iran à des stratagèmes complexes pour contourner les sanctions, notamment en occultant la BOI, afin de se procurer des biens à double usage pour son programme d'armes de destruction massive. On observe souvent que l'Iran utilise des sociétés écrans enregistrées dans des centres financiers clés pour transférer des fonds provenant de plateformes de change contrôlées par le gouvernement iranien.

Encadré 14. Étude de cas : Utilisation de prestataires de services de transport illégaux pour le commerce de biens à double usage

Des citoyens iraniens ont créé aux Pays-Bas plusieurs entités juridiques actives dans le secteur technologique. Cela implique le recours à une société de référence reconnue38.
(RRC) vise à faciliter l'obtention d'un permis de séjour néerlandais pour les migrants hautement qualifiés. Le RRC est également membre ou directement lié à un prestataire de services de placement immobilier illégal, qui fournit divers services tels que l'immatriculation d'une société, l'ouverture d'un compte bancaire et la vérification qu'au moins la moitié des dirigeants de la société sont de nationalité néerlandaise (afin de bénéficier des avantages fiscaux et des conventions fiscales néerlandaises).

Alors que les prestataires de services de fiducie légaux sont sous la supervision de la Banque centrale néerlandaise, les prestataires de services de fiducie illégaux répartissent leurs services au sein de plusieurs entités juridiques. Ce faisant, ces services sont moins chers et il devient plus difficile de les identifier. Par conséquent, la Banque centrale néerlandaise a du mal à superviser ces entités. Dans ce cas précis, des fonds prétendument en provenance d'Iran via d'importantes places financières sont transférés illégalement vers les entités juridiques néerlandaises créées par le prestataire de services de fiducie illégal. Ces fonds sont ensuite transférés au sein de cette structure et parviennent finalement aux migrants hautement qualifiés.

Dans ce cas, les relevés bancaires font état de multiples transactions qui constituent un risque pour l'approvisionnement de biens à double usage en Iran. Ces biens sont également susceptibles d'être utilisés à des fins de prolifération. Ces transactions concernent également les entreprises technologiques contrôlées par les migrants iraniens hautement qualifiés. On peut donc en conclure que ces entreprises agissent comme des sociétés écrans. Le recours à des prestataires de services de transaction, notamment illégaux, et la constitution d'un réseau d'entreprises rendent la détection de ces transactions financières extrêmement difficile.

Source : Pays-Bas

71. Les ESM non agréées sont également utilisées pour transférer des fonds au profit d'individus agissant pour le compte de groupes terroristes nationaux et désignés comme tels par l'ONU. Dans le cas ci-dessous, les autorités des Émirats arabes unis ont découvert un système complexe visant à utiliser une société écran comme hawaladar39 pour transférer des millions de dollars. Bien qu'il s'agisse d'un exemple d'individus échappant aux sanctions financières pour le compte d'acteurs non étatiques, il pourrait également s'appliquer aux types de systèmes complexes utilisés pour contourner les sanctions liées au PF.

Une référence reconnue est une entreprise, une école ou un organisme qui bénéficie de l'arrivée d'étrangers .
39 Hawaladar est un émetteur d'argent qui fournit des services Hawala.

Encadré 15. Étude de cas : Un MSB non agréé utilisé pour échapper aux sanctions contre un groupe terroriste figurant sur la liste 1267 de l'ONU

Au premier trimestre 2022, une maison de change locale a déposé une demande d'alerte/de signalement auprès de l'UAEFIU concernant des virements électroniques provenant d'une juridiction à haut risque et reçus par un résident étranger des Émirats arabes unis. Toutes les parties impliquées dans ces virements ont fait l'objet d'informations de renseignement financier obtenues par l'UAEFIU.

Selon l'enquête et l'analyse de l'UAEFIU, le principal suspect a reçu sept virements électroniques totalisant 3,5 millions de dollars américains et a créé une société écran aux Émirats arabes unis pour fonctionner comme hawaladar pour le transfert de fonds vers des pays à haut risque.
Soutenir les membres de Daech (EIIL) et du Front al-Nosra. Ces deux groupes figurent sur la liste nationale des Émirats arabes unis et sur la liste récapitulative des Nations unies (RCSNU 1267/1989).

L'UAEFIU a transmis à la Sûreté de l'État un dossier contenant des informations détaillées sur le suspect et sa société écran. En collaboration avec l'UAEFIU et la Banque centrale, la Sûreté de l'État a enquêté sur les activités financières du suspect. En conséquence, la Sûreté de l'État a émis une ordonnance de gel des fonds et autres actifs du suspect, pour un total de 500 000 dollars américains et 4 kg d'or. L'activité commerciale de la société écran a également été suspendue. Tout au long de l'enquête, le suspect a avoué avoir fourni des fonds à Daech (EIIL) et à Jabhat Al Nusra pour acquérir du matériel militaire, notamment des armes et des munitions.

Source : Émirats arabes unis

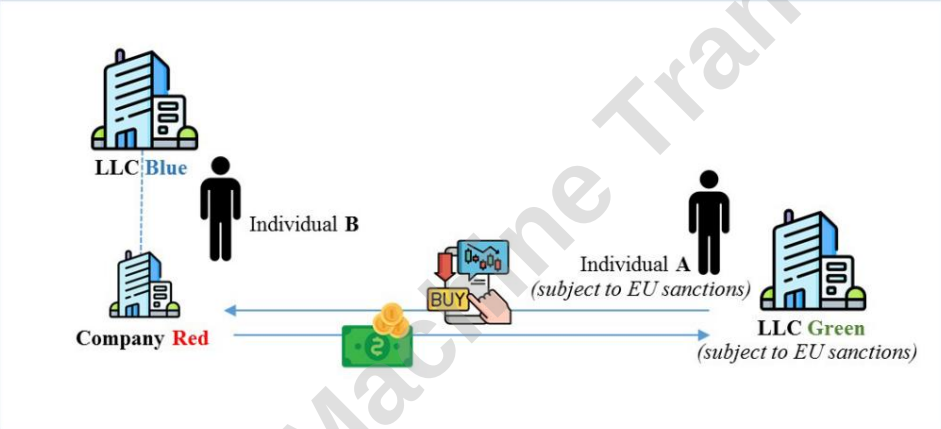
Utilisation de différents types de personnes morales pour échapper aux sanctions

72. Certains pays ont signalé le recours à des filiales et autres personnes morales pour brouiller les informations sur les véritables bénéficiaires effectifs. Parmi les tactiques courantes, on trouve des exemples de stratagèmes complexes visant à échapper aux sanctions et des approches plus directes pour cibler des secteurs dépourvus de contrôles stricts en matière de LBC/FT/CPF.

Encadré 16. Étude de cas : Un stratagème complexe pour échapper aux sanctions de l'UE

L'individu A, soumis aux sanctions de l'UE, a coordonné un stratagème complexe avec l'individu B pour faciliter l'évasion des sanctions. Premièrement, l'individu B, propriétaire de la société à responsabilité limitée (SARL) Blue, a créé une filiale appelée Company Red. Deuxièmement, l'individu B a utilisé Company Red pour acquérir la part de l'individu A dans LLC Green. Bien que LLC Green détienne 28,5 millions d'actions d'une société européenne, ces actions ont été gelées car LLC Green était contrôlée par l'individu A. Ainsi, lorsque Company Red a acquis la part de l'individu A dans LLC Green, elle a également acquis les actions gelées de la société européenne. En échange de la vente de LLC Green, l'individu A a reçu un avantage économique équivalent.

L'individu B a facilité l'évasion des sanctions parce que lui et les sociétés basées en Russie (LLC Blue, Company Red et LLC Green) ont utilisé ce stratagème pour vendre une société non européenne contrôlée par une personne inscrite sur la liste et possédant des actions gelées d'une société de l'UE dans le seul but de lever le gel de ces actions dans l'Union européenne.



Source : Commission européenne

Encadré 17. Étude de cas : Structure de propriété complexe utilisée pour dissimuler le véritable propriétaire des véhicules

Plusieurs sociétés écrans ont été utilisées pour dissimuler le véritable propriétaire de plusieurs véhicules de luxe d'une valeur de plusieurs centaines de milliers d'euros. La dernière société de la chaîne, Une SARL immatriculée en Allemagne était propriétaire des véhicules de luxe. Bien que la SARL ait officiellement pour mission de gérer ces véhicules, des enquêtes approfondies menées par l'Office central de l'application des sanctions ont permis de prouver que la société servait exclusivement à dissimuler la véritable propriété des véhicules.

En réalité, la société, et donc les véhicules, étaient contrôlés par une personne inscrite sur la liste des sanctions de l'UE contre la Russie. Après que l'enquête a révélé ce lien entre la personne inscrite et la SARL, les véhicules ont dû être gelés. Des investigations plus poussées ont permis d'attribuer d'autres actifs à la personne inscrite.

Source : Allemagne

Encadré 18. Étude de cas : Utilisation d'une filiale pour masquer un lien avec une entité de la RPDC désignée par l'ONU

La société BETA opère dans le secteur du bâtiment et des travaux publics, notamment en fournissant des engins lourds, des grues fixes et mobiles, des excavatrices, des chargeuses et des camions à d'autres entreprises. Ses principaux clients sont la société GAMMA et plusieurs PME du même secteur. Le propriétaire effectif de BETA, M. X, et le gérant, M. Y, sont tous deux ressortissants de la RPDC, pays soumis à des sanctions de l'ONU.

La société GAMMA, active dans le secteur agroalimentaire, a acheté des machines agroalimentaires à la société BETA. Après que cette dernière a encaissé un nombre inhabituel de chèques de plus de 300 000 € (200 000 000 francs CFA), une institution financière sénégalaise a mené des enquêtes de vigilance à l'égard de la clientèle, qui ont révélé que la société mère de BETA, basée à Pyongyang en RPDC, figure sur la liste des sanctions 1718 des Nations Unies.

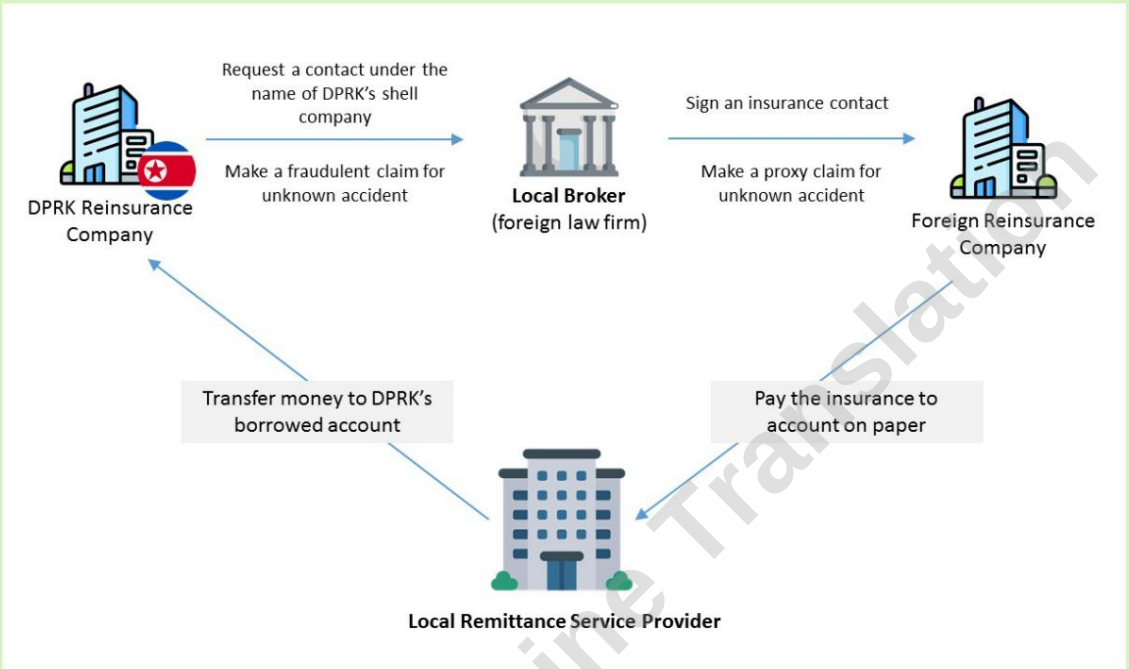
Après vérification du lien avec l'entité sanctionnée, l'institution financière a déposé une déclaration d'opération suspecte auprès de la CENTIF sénégalaise et les avoirs de la société BETA ont été gelés. Le STR a permis à la CENTIF de mener des enquêtes, qui n'ont pas révélé l'implication consciente de GAMMA dans le système d'évasion des sanctions.

Source : Sénégal

73. La RPDC gagne des millions de dollars chaque année en fabriquant des accidents et en escroquant le marché international de l'assurance. Faute de pouvoir vérifier les déclarations de sinistre en Corée du Nord, les compagnies de réassurance nord-coréennes souscrivent des assurances ou des réassurances internationales pour toutes les infrastructures publiques, telles que les ponts et les usines, puis falsifient ces assurances.

Documents pour percevoir les primes d'assurance. La RPDC mobilise des sociétés écrans ou des comptes empruntés afin de signer des contrats de réassurance et de percevoir les primes d'assurance.40

Encadré 19. Exemple illustratif : Utilisation par la RPDC de structures juridiques opaques pour commettre des fraudes à l'assurance



Exploitation des cartes de crédit et de débit par la RPDC

74. Plusieurs pays sont conscients que des individus associés à la RPDC obscurcissent de plus en plus leurs profils financiers en utilisant des comptes obtenus illégalement au nom de ressortissants chinois et en exploitant des actifs virtuels pour effectuer des paiements et accéder à la monnaie locale, permettant ainsi à la RPDC de continuer à contourner les sanctions de l'ONU.

75. On soupçonne que des banquiers de la RPDC gèrent frauduleusement de nombreuses cartes de débit UnionPay obtenues illégalement et émises par de grandes banques commerciales basées en Chine, au nom de centaines de titulaires de comptes nationaux, pour effectuer des paiements en monnaie locale. Il semble qu'il s'agisse d'une tentative de contournement des sanctions en masquant les transactions et les liens avec la RPDC, tout en contournant les pays appliquant de sévères sanctions contre la RPDC pour encaisser des bénéfices et acheter des articles interdits.

76. La nature apparemment décentralisée de ces réseaux financiers réduit également l'impact de toute perturbation individuelle et complique considérablement l'identification de tous les comptes de la RPDC par les autorités gouvernementales. Certains éléments indiquent que la RPDC utilise des cartes de débit UnionPay obtenues illégalement pour recevoir des dépôts de monnaie fiduciaire issue de cryptomonnaies volées, et coordonne les transactions pour diverses entités liées aux armes de destruction massive.

40 L'assurance et/ou la réassurance pour la RPDC constituent une violation des articles 33 et 36 de la résolution 2270 du Conseil de sécurité des Nations Unies, qui interdit aux États de fournir des liquidités, de l'or et des services d'assurance en vrac qui pourraient contribuer aux programmes nucléaires ou de missiles balistiques de la RPDC.

Typologie 3 : Utilisation d'actifs virtuels et d'autres technologies

77. On observe une tendance croissante à l'exploitation de l'économie numérique par des acteurs sanctionnés. Les actifs virtuels et autres nouvelles technologies sont utilisés pour contourner les régimes de sanctions internationaux, supranationaux et nationaux et financer les acteurs et les activités liés aux ADM.41 Les actifs virtuels sont utilisés pour faciliter les flux financiers :

un) directement aux pays sanctionnés ; et

b) indirectement par l'intermédiaire de pays tiers qui n'appliquent pas la sanction mesures. Par conséquent, la plupart des pays identifient l'utilisation d'actifs virtuels et d'autres nouvelles technologies par des acteurs illicites comme des menaces/vulnérabilités clés du PF.

78. Plus généralement, les pays ont également identifié les problèmes de contournement des sanctions découlant d'autres technologies émergentes telles que l'intelligence artificielle. Cependant, les données et les tendances dans ce domaine sont encore trop récentes pour permettre de tirer des conclusions, et peu d'études de cas sont disponibles.

Défis réglementaires

79. Malgré les efforts déployés pour lutter contre les risques émergents liés aux actifs virtuels et autres technologies, les PSAV de nombreux pays ne respectent pas les exigences en matière de LBC/FT. En avril 2024, les trois quarts des pays du Réseau mondial du GAFI étaient jugés non conformes ou partiellement conformes aux normes internationales relatives aux actifs virtuels et aux PSAV.42 Les lacunes de la réglementation et de la supervision à l'échelle internationale ont exposé le secteur aux abus des réseaux de FP. Tant qu'il existe des lacunes dans la mise en œuvre des normes du GAFI relatives aux actifs virtuels et aux PSAV entre les juridictions, les réseaux de FP peuvent recourir à des PSAV dans des juridictions dont les cadres sont faibles ou inexistants sans être détectés ni perturbés. Comme l'illustre le cas ci-dessous, il existe également des cas de PSAV soumis aux cadres de LBC/FT qui ne respectent pas les exigences applicables.

Encadré 20. Étude de cas : Mesures d'application de la loi Binance

En novembre 2023, Binance Holdings Limited (« Binance ») a plaidé coupable et accepté de payer plus de 4 milliards de dollars pour clore l'enquête du ministère américain de la Justice sur des violations liées à de multiples programmes de sanctions, notamment le défaut d'enregistrement en tant qu'entreprise de transfert de fonds et des violations de la loi sur les pouvoirs économiques d'urgence internationaux (IEEPA). Le fondateur et PDG de Binance a plaidé coupable de ne pas avoir maintenu un programme efficace de lutte contre le blanchiment d'argent, en violation de la loi sur le secret bancaire. (BSA).

En partie à cause de l'incapacité de Binance à mettre en œuvre un programme efficace de lutte contre le blanchiment d'argent, les acteurs illicites ont utilisé la bourse de Binance de diverses manières, notamment en effectuant des transactions qui ont masqué la source et la propriété des actifs virtuels ; en transférant les produits illicites des variantes de ransomware ; et en déplaçant les produits des transactions du marché darknet, des piratages d'échange et de diverses escroqueries liées à Internet.

41 Lors du Forum consultatif du secteur privé de mars 2025 en Inde, les participants ont souligné les risques accrus associés aux technologies financières émergentes, en particulier l'utilisation d'actifs virtuels dans les vols cybernétiques par des acteurs étatiques, y compris la RPDC, qui utilise des méthodes de plus en plus complexes et sophistiquées.

42 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

Les utilisateurs de Binance ont effectué des transactions avec des plateformes d'échange d'actifs virtuels dans des pays sanctionnés par les États-Unis, comme l'Iran, sans déposer de SAR/STR. Les portefeuilles des utilisateurs de Binance ont effectué un volume important de transactions directes avec diverses plateformes d'échange d'actifs virtuels iraniennes, d'une valeur de plus de 2 000 dollars chacune, soit l'équivalent de plus d'un demi-milliard de dollars au total. dollars. Ce total comprend également plusieurs transactions avec des portefeuilles d'actifs virtuels associés à des entités et des individus sanctionnés.

Source : États-Unis

Utilisation d'actifs virtuels pour déplacer des fonds

Les actifs virtuels sont utilisés pour dissimuler les mouvements de fonds vers 80 pays sanctionnés et leurs acteurs affiliés. Associés à certaines techniques, ils offrent un niveau d'anonymat plus élevé aux utilisateurs et peuvent être transférés instantanément au-delà des frontières. De plus, leur caractère international peut poser des difficultés liées à la vérification des juridictions où sont basés les PSAV étrangers, au temps et aux ressources nécessaires à la coopération internationale, ainsi qu'aux différences entre les cadres réglementaires et les régimes de sanctions d'une juridiction à l'autre. En particulier, les exemples présentés par les pays ont montré l'utilisation courante de portefeuilles d'actifs virtuels et de plateformes d'échange pour contourner les sanctions.

Encadré 21. Étude de cas : Fonds transférés à un VASP agréé au niveau national

Dans le cadre d'une étude plus large sur l'utilisation des nouvelles technologies pour le blanchiment d'argent et l'évasion des sanctions, la FIU d'Ukraine a découvert des mouvements suspects de fonds entre des échanges de crypto-monnaies, y compris un VASP sanctionné au niveau national.

La CRF a constaté qu'une plateforme d'échange de cryptomonnaies (la plateforme A), composée de sociétés enregistrées en Europe et dans d'autres pays (dont les Îles Vierges britanniques, Hong Kong, le Royaume-Uni et l'Estonie), recevait des actifs virtuels de deux autres plateformes d'échange de cryptomonnaies à haut risque (les plateformes B et C). Bien que le propriétaire de la plateforme A soit un ressortissant estonien, cette affaire intéressait la CRF ukrainienne, car le propriétaire était considéré comme un PPE ukrainien et fils d'un homme politique ukrainien.

La plateforme A recevait d'importants montants de fonds des plateformes B et C. La plateforme B a été identifiée comme un fournisseur de services d'investissement virtuels (VASP) russe sanctionné par l'Ukraine en vertu de son régime de sanctions nationales en 2023. La plateforme C a été identifiée comme une plateforme à haut risque, dont les propriétaires ont été arrêtés, soupçonnés de blanchiment de 700 millions de dollars. La CRF ukrainienne note que les plateformes B et C ont transféré des actifs virtuels via la blockchain Tron vers la plateforme d'échange cryptographique A afin de dissimuler l'origine et le mouvement des fonds.

Les conclusions de la FIU sont actuellement examinées dans le cadre d'une enquête préliminaire.

Source : Ukraine

Encadré 22. Étude de cas : Utilisation de diverses méthodes pour transférer des fonds vers la RPDC

En décembre 2024, la Corée du Sud a sanctionné une entité et 15 individus, dont Kim Chol Min et Kim Ryu Song, tous deux directeurs généraux du Bureau général 313 situé dans un pays voisin, pour avoir généré des fonds, lancé des cyberattaques et volé des actifs virtuels au nom de la RPDC.[43] Avec l'aide de facilitateurs du pays voisin, la RPDC a utilisé des portefeuilles virtuels, des banques, des plateformes de finance électronique et d'autres comptes en monnaie fiduciaire pour transférer des fonds. Après avoir converti une partie des produits illicites en monnaie fiduciaire, la RPDC a envoyé une importante somme d'argent à Pyongyang et a utilisé les revenus en monnaie fiduciaire provenant des actifs virtuels convertis pour acheter des fournitures sanctionnées et financer le programme d'armes de destruction massive du régime.

Le Bureau général 313 contrôle la recherche et le développement de la RPDC en matière d'armes et d'autres équipements militaires. Il participe également au déploiement des équipes informatiques de la RPDC dans les pays voisins et à l'international.

Source : Corée du Sud

81. Les acteurs liés au PF et à l'évasion des sanctions utilisent des méthodes de plus en plus sophistiquées pour blanchir des produits illicites via des actifs virtuels et masquer les sources de financement.
Des pays comme la RPDC mènent cette activité au moyen de technologies améliorant l'anonymat, comme les mixers, les systèmes de finance prétendument décentralisée (DeFi), les passerelles inter-chaînes, ainsi que les VASP sans contrôles LBC/FT. Après avoir blanchi des fonds, les acteurs de l'évasion des sanctions convertissent souvent des actifs virtuels en monnaie fiduciaire auprès de courtiers de gré à gré (OTC) concentrés dans certaines juridictions.44 Dans certains cas, la RPDC demande aux courtiers de gré à gré d'envoyer les fonds convertis sur des comptes bancaires détenus par des sociétés écrans, qui achètent des biens pour le compte de la RPDC. Comme indiqué précédemment, dans certains cas, la RPDC utilise des cartes de débit UnionPay obtenues illégalement pour recevoir des dépôts de monnaie fiduciaire provenant d'actifs virtuels volés.

Encadré 23. Étude de cas : Désignation des personnes chargées de blanchir des fonds aux fins de sanctions

En novembre 2023, l'OFAC a désigné des mixeurs impliqués dans le blanchiment de fonds pour la RPDC, dont Sinbad.io (Sinbad).45 Sinbad a servi d'outil clé de blanchiment d'argent pour le groupe Lazarus, un groupe de pirates informatiques parrainé par la RPDC. Sinbad a traité des millions de dollars d'actifs virtuels que le groupe Lazarus avait volés, notamment lors des braquages très médiatisés d'Horizon Bridge, d'Axie Infinity et d'Atomic Wallet. À l'instar de Blender.io, Sinbad opérait sur la blockchain Bitcoin et facilitait sans discernement des transactions illégales en masquant leur origine, leur destination et leurs contreparties.

Source : États-Unis

43 https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=375771
44 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-actifs-virtuels-vasps-2024.html

Encadré 24. Étude de cas : Poursuites pénales et mesures d'application connexes en RPDC

En avril 2023, le ministère de la Justice a rendu public deux actes d'accusation accusant un représentant du FTB de RPDC pour son rôle dans des complots de blanchiment d'argent visant à générer des revenus pour la RPDC grâce à des actifs virtuels. L'individu aurait conspiré avec deux traders de gré à gré pour blanchir des actifs virtuels volés et aurait utilisé ces fonds pour acheter des biens en dollars américains pour le compte du gouvernement de la RPDC via des sociétés écrans basées à Hong Kong.

L'OFAC a également désigné l'individu ayant reçu des dizaines de millions de dollars en actifs virtuels, provenant en partie de personnes de RPDC recrutées à leur insu par des entreprises américaines pour effectuer des travaux de développement informatique. Lorsque ces informaticiens obtiennent un emploi, ils sont connus pour demander à être payés en actifs virtuels et pour reverser la majeure partie de leurs salaires via un système de blanchiment complexe afin de réacheminer ces fonds illégalement obtenus vers la RPDC. Après avoir apparemment reçu de l'argent de développeurs informatiques, le représentant du FTB a demandé aux négociants en actifs virtuels de gré à gré d'envoyer des paiements à des sociétés écrans, afin que celles-ci puissent effectuer des paiements en monnaie fiduciaire pour des biens, tels que du tabac et des appareils de communication, au nom du régime de la RPDC.
Cette action est le fruit d'une collaboration continue entre l'OFAC, le ministère de la Justice et le FBI. Elle a également été menée en étroite coordination avec la République de Corée, qui a désigné le même individu pour ses activités illicites.

Source : États-Unis

Les AV et la génération de fonds

82. Certains pays ont constaté que la RPDC recourait au vol d'actifs virtuels et aux cyberattaques pour lever des fonds à l'échelle mondiale, notamment pour ses programmes d'armes de destruction massive et de missiles balistiques. Lors de la réalisation de cette activité, la RPDC et les acteurs associés ciblent généralement les organisations du secteur de la technologie blockchain et des actifs virtuels, notamment les VASP, les services DeFi, les développeurs de ponts blockchain, les sociétés de négoce d'actifs virtuels et les fonds de capital-risque investissant dans les actifs virtuels.

83. En 2024, un rapport d'un groupe d'experts de l'ONU sur la RPDC a mis en évidence une cyberactivité mondiale au nom du régime de la RPDC, où ils enquêtaient sur un total de 58 cyberattaques présumées de la RPDC contre des sociétés liées aux actifs virtuels entre 2017 et 2023, évaluées à environ 3 milliards de dollars.[46] Selon Chainalysis, des pirates informatiques liés à la RPDC ont volé environ 428,8 millions de dollars aux plateformes DeFi en 2023, et ont également ciblé des services centralisés (150 millions de dollars volés), des échanges (330,9 millions de dollars) et des fournisseurs de portefeuilles (127 millions de dollars).[47] Les pays ont également souligné le déploiement frauduleux par la RPDC de travailleurs des services informatiques pour générer des fonds (dans certains cas en recevant des paiements en actifs virtuels) et échapper aux sanctions. Les acteurs de la RPDC utilisent les méthodes décrites dans la section ci-dessus pour blanchir les produits générés par les actifs virtuels.

46 S/2024/215 47
Rapport sur la criminalité cryptographique 2024 de Chainalysis (pages 44-46) Étude de cas Exploit du portefeuille atomique de la RPDC.

Encadré 25. Étude de cas : Vol et fraude par cybercriminalité

En février 2021, le ministère de la Justice a accusé trois programmeurs informatiques de la RPDC d'avoir participé à une vaste conspiration criminelle visant à mener une série de cyberattaques destructrices, à voler et à extorquer plus de 1,3 milliard de dollars d'argent et de cryptomonnaies à des institutions financières et à des entreprises, à créer et à déployer plusieurs applications de cryptomonnaies malveillantes et à développer et commercialiser frauduleusement une plateforme blockchain.

L'acte d'accusation allègue que les trois accusés étaient membres d'unités du Bureau général de reconnaissance (RGB), une agence de renseignement militaire de la RPDC, qui se livraient à des activités de piratage informatique criminelles48. Ces unités de piratage militaire de la RPDC sont connues sous plusieurs noms dans la communauté de la cybersécurité, notamment Lazarus Group et Advanced Persistent Threat 38 (APT38).

L'acte d'accusation allègue un large éventail d'activités cybercriminelles menées par le complot, aux États-Unis et à l'étranger, à des fins de vengeance ou de profit. Les stratagèmes allégués comprennent la création et le déploiement d'applications malveillantes de cryptomonnaies ; le ciblage d'entreprises de cryptomonnaies et le vol de cryptomonnaies ; des campagnes de spear-phishing ; et l'émission de jetons de chaîne marine et d'offres initiales de cryptomonnaies.

Selon les allégations contenues dans l'acte d'accusation, les trois accusés étaient membres d'unités du RGB, stationnées par le gouvernement de la RPDC dans d'autres pays, notamment en Chine et en Russie. Bien que ces accusés fassent partie des unités du RGB, désignées par les chercheurs en cybersécurité sous les noms de Groupe Lazarus et APT 38, l'acte d'accusation allègue que ces groupes ont participé à un complot commun visant à causer des dommages, à voler des données et de l'argent, et à promouvoir les intérêts stratégiques et financiers de la RPDC.

Les ministères du Trésor et de la Justice ont également engagé des poursuites contre deux ressortissants chinois accusés d'avoir blanchi plus de 100 millions de dollars de cryptomonnaies suite au piratage d'une plateforme d'échange de cryptomonnaies. Selon les plaidoiries, en 2018, des complices de la RPDC ont piraté une plateforme d'échange de cryptomonnaies et ont volé près de 250 millions de dollars de cryptomonnaies. Les fonds ont ensuite été blanchis via des centaines de transactions automatisées de cryptomonnaies visant à empêcher les forces de l'ordre de les retrouver. Les plaidoiries allèguent en outre qu'entre décembre 2017 et avril 2019, les deux accusés ont blanchi plus de 100 millions de dollars de cryptomonnaies, provenant principalement du piratage de plateformes d'échange de cryptomonnaies. L'OFAC a désigné les deux individus pour avoir fourni un soutien matériel au groupe Lazarus.

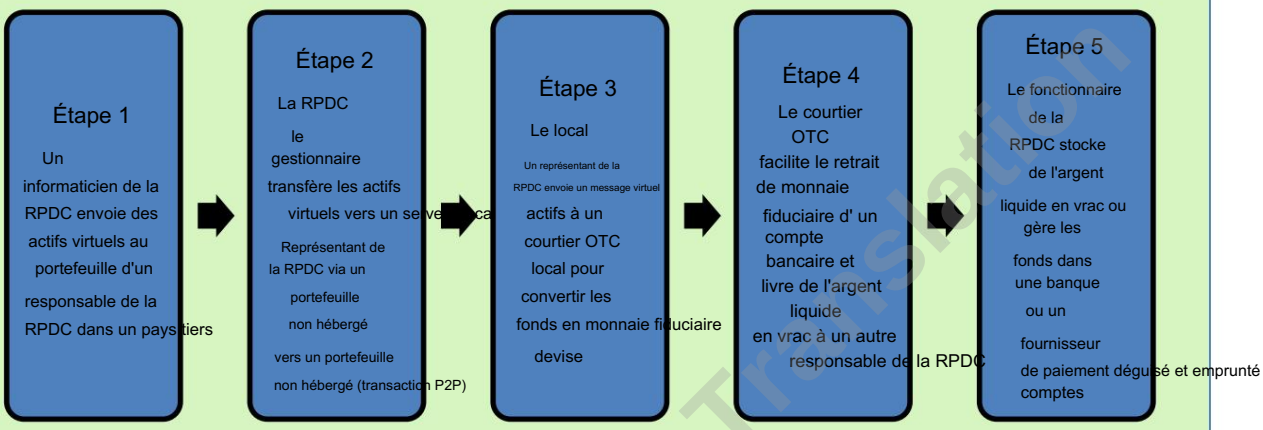
Source : États-Unis

84. De plus, la RPDC a déployé des milliers d'informaticiens hautement qualifiés à travers le monde afin de générer des revenus, contribuant ainsi à ses programmes d'armes de destruction massive et de missiles balistiques. Ces informaticiens exploitent la demande existante de compétences informatiques spécifiques, comme le développement de logiciels et d'applications mobiles, pour obtenir des contrats de travail en freelance auprès de clients du monde entier, notamment en Asie, en Europe et en Amérique du Nord. Dans de nombreux cas, les informaticiens de RPDC se présentent comme des télétravailleurs basés à l'étranger et/ou non originaires de RPDC. Les informaticiens de RPDC qui obtiennent les projets utilisent le profil du facilitateur.

Sur la liste de la résolution 1718 du Conseil de sécurité des Nations Unies, le RGB est désigné par KPe.031.

L'identité des personnes concernées peut être encore plus obscurcie par la sous-traitance des projets. L'argent est renvoyé en RPDC par divers moyens pour échapper aux sanctions, notamment par le recours à des intermédiaires et en occultant la BOI (voir typologies 1 et 2).
Les actifs virtuels sont également utilisés pour transférer des fonds vers la RPDC.

Encadré 26. Exemple illustratif : Processus de transfert de fonds illicites d'un informaticien de la RPDC



Entités et individus étrangers commettant des fraudes pour dissimuler des activités lucratives avec

Travailleurs informatiques de la RPDC

85. En outre, les informaticiens de la RPDC cooptent également des personnes et des entreprises étrangères pour masquer davantage leur implication dans des stratagèmes d'évasion des sanctions à des fins lucratives.
Dans les études de cas ci-dessous, des entreprises japonaises ont été ciblées par des informaticiens liés à la RPDC pour lever et transférer des fonds. Dans l'autre étude de cas, un ressortissant américain a participé à un stratagème comprenant du blanchiment d'argent et de l'usurpation d'identité pour soutenir des informaticiens de la RPDC.

Encadré 27. Étude de cas : Des stratagèmes frauduleux visant à masquer des relations commerciales lucratives avec des informaticiens de la RPDC

En mars 2024, un ressortissant sud-coréen, président d'une entreprise informatique et ancien employé, ont été arrêtés pour fraude et autres délits. L'enquête a révélé que les suspects avaient falsifié des documents et demandé à des informaticiens de RPDC, vraisemblablement basés en Chine, de développer des applications commandées par une entreprise japonaise via une plateforme en ligne. Cette activité présumée était soupçonnée de soutenir un stratagème visant à contourner les sanctions, ces fonds pouvant être utilisés pour financer le programme d'armes de destruction massive de la RPDC, en violation de la résolution 1718 du Conseil de sécurité des Nations unies.

En septembre 2024, deux Japonais ont été arrêtés pour avoir conspiré avec un informaticien présumé de la RPDC afin d'utiliser un système de trading automatique interdit pour effectuer des transactions de change, et pour s'être inscrits illégalement dans la base de données clients et avoir ouvert des comptes. Les suspects sont soupçonnés d'avoir transféré des fonds obtenus grâce à ces transactions de change illégales vers la Corée du Nord.

Source : Japon

Encadré 28 : Le ministère américain de la Justice démantèle les stratagèmes de fraude visant les travailleurs informatiques à distance de la RPDC en inculpant et en arrêtant un facilitateur de Nashville

En août 2024, le ministère de la Justice a rendu public un acte d'accusation accusant un ressortissant américain de complot en vue de blanchir des instruments financiers et de plusieurs autres crimes visant à générer des revenus pour le programme d'armement illicite de la RPDC, dont des armes de destruction massive. Selon les documents judiciaires, le défendeur aurait participé à un stratagème visant à aider des informaticiens étrangers à obtenir du travail informatique à distance dans des entreprises américaines, qui pensaient recruter du personnel basé aux États-Unis.
Les travailleurs informatiques, qui étaient des ressortissants de la RPDC, ont utilisé l'identité volée d'un citoyen américain pour obtenir ce travail informatique à distance.

Selon les documents judiciaires, le défendeur a exploité une « ferme d'ordinateurs portables » à ses résidences de Nashville entre juillet 2022 et août 2023 environ. Les entreprises victimes ont expédié des ordinateurs portables adressés à « Andrew M. » aux résidences du défendeur. Après réception des ordinateurs, le défendeur a téléchargé et installé des applications de bureau à distance non autorisées et a accédé aux réseaux des entreprises victimes, endommageant les ordinateurs. Ces applications ont permis aux informaticiens de RPDC de travailler depuis des sites en Chine, tout en laissant croire aux entreprises victimes qu'« Andrew M. » travaillait depuis les résidences du défendeur à Nashville.

Les informaticiens étrangers associés à la ferme d'ordinateurs portables du défendeur ont perçu plus de 250 000 dollars pour leur travail entre juillet 2022 et août 2023 environ, dont une grande partie a été faussement déclarée à l'Internal Revenue Service (IRS) et à la Social Security Administration (SSIA) des États-Unis au nom de la personne américaine dont l'identité a été usurpée. Les agissements du défendeur et de ses complices ont également occasionné aux entreprises victimes plus de 500 000 dollars de frais liés à l'audit et à la remise en état de leurs appareils, systèmes et réseaux. Le défendeur et d'autres personnes ont conspiré pour blanchir de l'argent en effectuant des transactions financières afin de recevoir des paiements des entreprises victimes et de transférer ces fonds au défendeur et sur des comptes situés hors des États-Unis, dans le but de promouvoir leurs activités illégales et de dissimuler que les fonds transférés en étaient le produit. Les comptes non américains incluent des comptes associés à la RPDC.

et des acteurs chinois.

Source : États-Unis

Typologie 4 : Exploiter les secteurs maritime et maritime

86. Selon la définition de l'Organisation maritime internationale (OMI), la flotte fantôme , ou flotte obscure, désigne « […] les navires se livrant à des opérations illégales afin de contourner les sanctions ou de se livrer à d'autres activités illégales […] ».49 Le secteur maritime est devenu une cible privilégiée des acteurs illicites, tirant parti de sa complexité, de sa portée internationale, de son anonymat et de ses contrôles limités en matière de LBC/FT/PCF. L'industrie maritime implique un vaste réseau de navires, de ports, de logistique et de réglementations internationales que les acteurs illicites peuvent exploiter pour échapper aux sanctions et générer des revenus susceptibles de contribuer au PF. Bien que les normes du GAFI ne couvrent pas le secteur maritime, plusieurs pays ont identifié l'utilisation de ce secteur comme une vulnérabilité majeure dans leur évaluation nationale des risques liés au PF. À cette fin, divers aspects et activités du secteur maritime sont potentiellement exposés au contournement des sanctions.

49 Organisation maritime internationale, « Exhortant les États membres et toutes les parties prenantes concernées à promouvoir des actions visant à prévenir les opérations illégales dans le secteur maritime par la « flotte noire » ou la « flotte fantôme » » (déc. 6, 2023). A 1192 33

et les risques PF, y compris les accords d'assurance maritime, les compagnies maritimes, les registres ouverts, les négociants en matières premières et les fabricants de biens à double usage.50

87. Les acteurs illicites peuvent employer toute une gamme de tactiques de navigation trompeuses pour dissimuler le navire, ses origines ou sa désignation, obscurcir la véritable nature de leurs activités et échapper à la détection. Bien que les techniques se chevauchent, les tactiques peuvent être divisées en quatre grandes catégories : l'identification des navires, les transferts de navire à navire, la désactivation ou le masquage des émissions AIS et la falsification de documents. Il est toutefois important de noter que les acteurs illicites qui tentent de contourner les sanctions et les PF peuvent employer plusieurs tactiques pour parvenir à leurs fins.

Modification de l'identification du navire

88. Comme indiqué dans la typologie 2, les acteurs illicites peuvent masquer les informations sur la propriété effective afin de contourner les régimes de sanctions et d'accéder au système financier formel. Dans le secteur maritime, ils peuvent modifier physiquement des navires marchands pour les faire passer pour d'autres véhicules et masquer leur identité afin de dissimuler leur véritable propriété et leurs activités. Par exemple, l'identité physique d'un navire peut être falsifiée en masquant son nom, en utilisant des pseudonymes et en modifiant son numéro d'identification OMI unique. En modifiant physiquement les navires marchands et en masquant leur identité, les acteurs illicites acquièrent l'anonymat et peuvent masquer l'historique des activités illégales d'un navire. L'étude de cas ci-dessous présente un exemple de navire modifiant son identification pour contourner les résolutions du Conseil de sécurité des Nations Unies sur la RPDC.

50 Pour aider les membres à se préparer aux évaluations mutuelles et à répondre aux risques régionaux émergents, le Le Secrétariat de l'APG, avec le soutien de l'Office des Nations Unies contre la drogue et le crime, a publié un document sur les expéditions. Fiche d'information sur les risques liés aux registres et aux fonds de pension : Groupe Asie-Pacifique sur le blanchiment d'argent

Encadré 29. Étude de cas : Génération de revenus grâce au charbon illicite dans le secteur maritime

En 2022, les autorités indonésiennes patrouillant dans les eaux indonésiennes ont arrêté le Petrel 8. En 2017, le Petrel 8, un vraquier sous pavillon des Comores, a été ajouté à la liste des sanctions de l'ONU pour avoir transporté du charbon illicite vers la RPDC. Cette affaire impliquait la coordination des autorités indonésiennes avec le Comité des sanctions 1718 de l'ONU. Le ministère indonésien des Affaires étrangères (MOFA) a demandé des informations à la Cellule de renseignement financier indonésienne (PPATK), ce qui a permis de détecter l'affaire grâce à la coopération internationale.

Français L'enquête a révélé que PT Lintas Bahari Nusantara, une société de transport maritime indonésienne, avait acheté le navire à une société japonaise, UYO Co. Ltd, pour un montant estimé à 500 000 yens, avec un financement fourni par la Banque BCA. Bien que l'enquête initiale n'ait pas identifié de liens financiers directs avec la RPDC, la détention du navire résultait de son implication dans le contournement continu des sanctions pour la RPDC. Des méthodes telles que la falsification de l'identité du navire et l'utilisation de pseudonymes ont été utilisées pour échapper à la détection. Le navire a été acheté pour environ 61 milliards de roupies (4 millions de dollars) et a été utilisé pour transporter du charbon vers la RPDC. L'acquisition du Petrel 8 a impliqué le transfert de fonds d'une société indonésienne à une entreprise japonaise.

Cette affaire a mis en lumière les vulnérabilités de la surveillance des changements de propriété des navires et des pratiques commerciales illicites, soulignant la nécessité d'une coopération internationale renforcée pour prévenir le contournement des sanctions. Suite aux discussions avec le Comité des sanctions 1718 de l'ONU en 2023, la décision de mettre au rebut le Petrel 8 a été jugée comme la solution la plus efficace pour prévenir de nouvelles activités de contournement des sanctions.

Source : Indonésie

Transferts de navire à navire

89. Le transfert de navire à navire se produit lorsque des marchandises sont déplacées entre navires en haute mer. Bien que ces transferts puissent être une pratique légitime, ils présentent un risque élevé de contournement des sanctions, car des acteurs illicites peuvent y recourir pour dissimuler l'origine ou la destination des expéditions. Il est donc plus difficile pour les autorités gouvernementales de suivre les marchandises sanctionnées et d'identifier les violations des sanctions internationales. De plus, le manque de transparence peut inciter les assureurs maritimes à fournir involontairement une assurance transport à des navires impliqués dans des activités illicites de transfert de navire à navire.

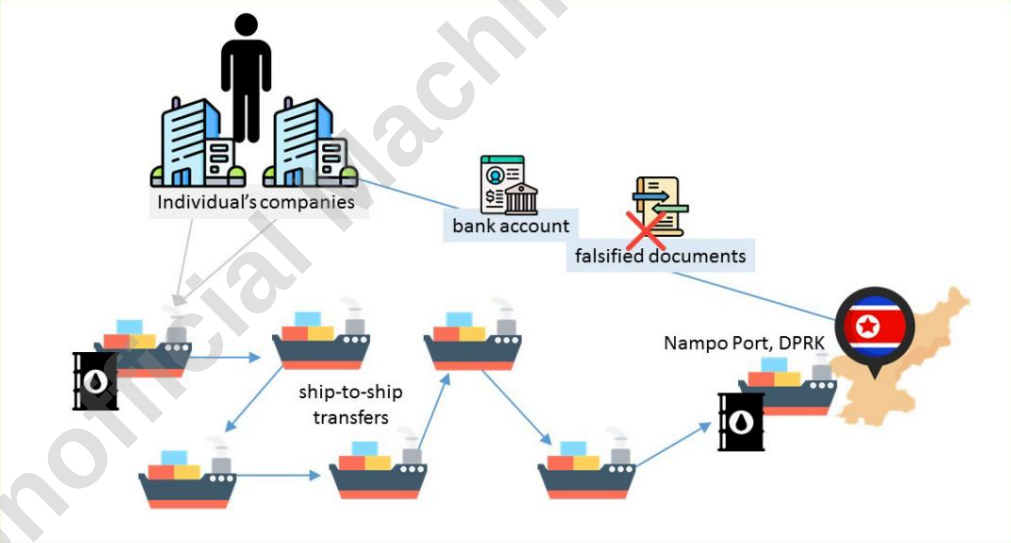
90. Selon une juridiction, la RPDC exploite une flotte d'au moins 28 pétroliers capables d'effectuer des transferts de produits pétroliers raffinés entre navires, et d'au moins 33 navires capables de transporter du charbon. Les transferts de navire à navire effectués par la RPDC sont souvent des transactions en espèces qui ne passent pas par des institutions financières, ce qui met en évidence une vulnérabilité supplémentaire liée au risque de fraude fiscale et de contournement des sanctions. Les études de cas ci-dessous détaillent comment les acteurs illicites peuvent utiliser les transferts de navire à navire pour transporter des articles interdits, contourner les sanctions et masquer la véritable origine ou destination afin d'éviter d'être détectés.

Encadré 30. Étude de cas : Exploiter le secteur maritime pour approvisionner la RPDC en gasoil

Fin 2019, un individu aurait conspiré avec cinq autres personnes à l'étranger pour fournir environ 12 260 tonnes de gasoil à la RPDC à bord du navire MT Courageous, à sept reprises. Les six premières fois, ces livraisons ont été facilitées par des transferts de navire à navire, le dernier ayant eu lieu au port de Nampo, en RPDC. Ces actes présumés constituent une violation du Règlement de Singapour sur la RPDC et du régime de sanctions de la résolution 1718 du Conseil de sécurité des Nations Unies.

Afin de faciliter les paiements pour l'achat et la fourniture de gasoil à la RPDC, l'individu est accusé d'avoir utilisé le compte bancaire d'une société dont il était administrateur à quatre reprises. Il aurait également falsifié des documents appartenant à la société à deux reprises et utilisé le compte bancaire d'une autre société sous son contrôle pour recevoir des paiements pour la fourniture interdite de gasoil à la RPDC à cinq reprises. De plus, l'accusé aurait menti à l'enquêteur, éliminé des preuves et omis d'informer la police de la fourniture de gasoil à la RPDC par un autre navire en février 2019.

Par conséquent, l'accusé fait face à de multiples chefs d'accusation, notamment de fourniture d'articles interdits à la RPDC, de falsification de comptes, d'obtention d'avantages découlant d'une conduite criminelle, d'entrave à la justice et de non-divulgation d'une transaction interdite. De plus, la première société dont l'accusé était administrateur a été inculpée de quatre chefs d'accusation de transfert d'actifs financiers susceptibles de contribuer à une activité interdite en violation du Règlement de Singapour sur la RPDC de l'ONU, et la seconde société fait face à cinq chefs d'accusation de profit découlant d'une conduite criminelle. La procédure judiciaire est en cours.



Source : Singapour

Encadré 31. Étude de cas : Transfert de pétrole aux navires de la RPDC en haute mer

De janvier 2017 à octobre 2022, les procureurs du Taipei chinois ont enquêté sur 11 cas impliquant des violations des sanctions par la RPDC.51 La typologie la plus courante impliquant le PF est le transfert de pétrole aux navires de la RPDC en haute mer à partir de navires de juridictions tierces contrôlés par des compagnies pétrolières du Taipei chinois, ou le transfert de pétrole à des navires appartenant à des juridictions tierces qui le revendent aux navires de la RPDC.

Les produits pétroliers demeurent la marchandise la plus fréquemment commercialisée par les habitants du Taipei chinois, en violation des sanctions de l'ONU. En vertu de la législation locale, le commerce du pétrole en haute mer est légal. Les représentants ou bénéficiaires effectifs de compagnies maritimes, y compris des ressortissants étrangers et d'autres intermédiaires, et impliquant des structures commerciales complexes, négocient des transactions apparemment légales pour dissimuler des transferts illicites de pétrole par des transferts de navire à navire en mer. De fausses informations d'exportation sont également utilisées, ainsi que des sociétés et des comptes offshore, pour entraver le traçage des fonds.52

Source : Taipei chinois

Désactivation et manipulation des diffusions du système d'identification automatisé

91. Le Système d'identification automatisé (SIA) est un système de suivi côtier utilisé à bord des navires pour fournir des informations d'identification et de positionnement, permettant aux autorités de suivre les mouvements.53 Les acteurs illicites peuvent manipuler les données transmises via les diffusions SIA, notamment en modifiant le nom des navires, les numéros OMI ou d'autres informations d'identification uniques, afin de dissimuler le voyage d'un navire. De plus, les flottes fantômes désactivent souvent la diffusion SIA, ce qui interrompt le suivi des mouvements.54

92. Comme indiqué par les pays et reflété dans la résolution 2397 (2017) du Conseil de sécurité des Nations Unies, les navires battant pavillon de la RPDC, contrôlés, affrétés ou exploités par elle désactivent ou manipulent intentionnellement les transpondeurs AIS pour échapper aux sanctions de l'ONU et générer des revenus qui ont historiquement contribué aux programmes d'armes de destruction massive et de missiles balistiques du pays55. L'étude de cas ci-dessous détaille deux incidents distincts de détection, de saisie et de confiscation de charbon originaire de la RPDC trouvé sur des navires civils, en violation des résolutions du Conseil de sécurité des Nations Unies relatives à la RPDC.

Cinq affaires ont abouti à des condamnations, trois ont été déclarées non coupables et trois n'ont pas donné lieu à des poursuites.

52 L'élément subjectif de l'article 9, paragraphe 1, alinéa 1 de la Loi sur la lutte contre le financement du terrorisme La loi exige qu'un suspect commerce « sciemment » avec la cible sanctionnée, et l'intervention d'intermédiaires a rendu cet élément difficile à prouver.

53 Organisation maritime internationale, « LIGNES DIRECTRICES RÉVISÉES POUR L'UTILISATION OPÉRATIONNELLE À BORD DES SYSTÈMES D'IDENTIFICATION AUTOMATIQUE (AIS) », (2 décembre 2015). A 1106 29

L'OMI impose l'utilisation de l'AIS pour tous les navires de plus de 300 tonneaux de jauge brute engagés dans des activités internationales. voyages, ainsi que tous les navires à passagers, quelle que soit leur taille.

55 Résolution 2397 du Conseil de sécurité des Nations Unies

Encadré 32. Étude de cas : Détection, saisie et confiscation de charbon provenant de la RPDC sur les navires

Lors de deux incidents distincts, le Cambodge a découvert que la RPDC utilisait des navires civils pour faciliter l'exportation de charbon, en violation des résolutions 2397 et 2375 du Conseil de sécurité des Nations unies, qui interdisent de telles activités. Dans les deux cas, les navires et leur cargaison ont été saisis, et les individus ont été reconnus coupables (1) d'entrée illégale au Cambodge et (2) de tentative de contrebande de marchandises dans la zone douanière du Cambodge.

Conformément aux obligations des Nations Unies, le Cambodge enquête et examine régulièrement les biens et les navires entrant par la haute mer afin de déceler d'éventuelles violations des sanctions des Nations Unies contre la RPDC. Parfois, les navires ont recours à des techniques d'obscurcissement pour dissimuler l'origine de leurs cargaisons, comme la désactivation de leur système d'identification automatique (AIS) pour masquer les marchandises à bord, la falsification de leur localisation ou les transferts de navire à navire. Deux saisies récentes de navires illustrent les tactiques employées par les navires de la RPDC pour masquer l'origine de leurs cargaisons illicites.

Dans le premier cas, le navire à moteur HJL a été saisi par les autorités cambodgiennes en février 2024. Après s'être approché des eaux de la RPDC, le navire, immatriculé à l'étranger, a désactivé son système AIS. Le lendemain, ce système a transmis une position indiquant que le HJL était ancré, alors même qu'il faisait toujours route sous un faux nom. Après son entrée dans les eaux territoriales cambodgiennes, les autorités cambodgiennes ont saisi le navire, avec l'aide d'une autre juridiction partageant des informations sur un navire suspect. Cette coopération internationale a conduit à la saisie du HJL, qui transportait 12 000 tonnes de minerai de charbon en provenance de la RPDC. Le navire est entré dans les eaux territoriales cambodgiennes pour jeter l'ancre, soi-disant à l'endroit où il rencontrerait ses acheteurs.

Conformément aux ordres permanents et en raison du contenu à bord, le parquet a gelé le navire et sa cargaison pour une enquête plus approfondie et un procès.

Dans le second cas, en mai 2024, les autorités cambodgiennes ont saisi le M/V CNI après qu'il ait effectué un transfert de navire à navire avec un navire de la RPDC dans les eaux de la RPDC, impliquant une cargaison interdite par l'ONU, dont 4 800 tonnes de minerai de charbon. Des enquêtes plus approfondies ont révélé que l'expédition avait été organisée par une société de logistique d'un pays tiers, et que cette société avait organisé l'importation de minerais de charbon originaires de la RPDC, tout en dissimulant son origine au moyen de documents falsifiés.

Source : Cambodge

93. Les vulnérabilités démontrées par les deux cas ci-dessus soulignent la nécessité pour les pays d'envisager d'accroître la fréquence de la surveillance et la présence des forces de patrouille, ainsi que de renforcer les systèmes de suivi dans les eaux territoriales, en particulier celles situées à proximité géographique des eaux internationales.

Falsification de documents

94. Une autre tactique visant à dissimuler l'origine ou la destination des marchandises consiste à utiliser de faux documents lors du transport de marchandises en provenance ou à destination de la RPDC, notamment pour les exportations de biens à double usage. Dans ce cas, les acteurs illicites falsifient les documents de transport d'une cargaison après son départ, dissimulant ainsi la véritable destination finale des marchandises. Cette pratique implique généralement une société écran dans un pays tiers, contrôlée plus ou moins directement par l'entité proliférante. Aux yeux des autorités douanières et de l'expéditeur, la société écran est le destinataire officiel de la cargaison. Cependant, une fois les marchandises reçues,

sont expédiés, le promoteur apporte une modification à la documentation de transport, permettant à l'envoi d'être redirigé vers une juridiction à haut risque associée au PF.

95. Outre la pratique de falsification de documents impliquant la RPDC, il s'agit d'une tactique courante pour contourner les sanctions et les contrôles à l'exportation dans d'autres pays. Les études de cas ci-dessous illustrent comment des acteurs illicites peuvent manipuler les documents de transport en amont du processus d'expédition pour dissimuler l'exportation de biens à double usage.

Encadré 33. Étude de cas : Falsification de factures et fausses déclarations d'expéditions à double usage

Lors du processus d'approbation des permis en 2021, l'Autorité fédérale de réglementation nucléaire (FANR) a identifié une cargaison suspecte contenant des biens à double usage. La société X, basée dans une zone franche des Émirats arabes unis, avait soumis trois permis d'exportation d'onduleurs d'une valeur d'environ 25 000 USD (95 040 AED). Les onduleurs figuraient sur la liste des marchandises contrôlées à l'exportation des Émirats arabes unis et étaient classés comme biens à double usage. Les documents soumis par la société X comprenaient un connaissement et un acte de vente et d'achat (BSP), qui contenaient des informations contradictoires concernant les coordonnées du vendeur et le pays d'origine de l'expédition. Les documents précisaient que ces articles étaient destinés à un pays à haut risque.

Les enquêtes des LEA ont permis d'identifier que la société X avait soumis un faux connaissement, se déclarant expéditeur, tandis que le BSP identifiait le vendeur comme une autre société située dans le pays T. Les LEA ont également déterminé, à la suite d'enquêtes complémentaires, que le vendeur présumé commercialisait principalement des noix et que, par conséquent, son activité n'était pas cohérente avec la transaction commerciale. Des enquêtes plus poussées ont révélé que les articles avaient en fait été importés par le vendeur du pays H vers les Émirats arabes unis. La société X a également fourni de faux documents attestant de l'existence de plusieurs succursales dans le pays U afin de tromper les autorités et d'échapper aux sanctions imposées au programme nucléaire iranien.

Les services répressifs ont mené une enquête criminelle et financière en coopération avec l'UAEFIU, la CBUAE, l'EOCN, l'Autorité fédérale des douanes et la FANR. Une inspection physique des locaux de la société X a révélé qu'elle opérait comme écran pour l'acheteur des onduleurs, situé dans un pays à haut risque. L'UAEFIU et la CBUAE ont identifié et gelé trois comptes bancaires d'un solde total de 34 000 AED (9 500 USD) liés à la société X.

En outre, les douanes ont fourni aux autorités policières et judiciaires tous les faux documents identifiés liés aux sous-traitants d'importation/exportation qui tentaient de masquer les informations de transaction.

FANR a préparé un rapport technique sur l'expédition et a fourni aux autorités locales de l'énergie (LEA) la confirmation que l'article est un bien à double usage figurant sur la liste de contrôle des exportations des Émirats arabes unis. Les autorités douanières ont saisi la cargaison et les forces de l'ordre ont ordonné son gel (95 040 AED (26 000 USD)).

Source : Émirats arabes unis

Encadré 34. Étude de cas : Non-déclaration de biens à double usage en vertu des lois d'exportation prescrites par le pays exportateur

En 2020, les autorités douanières indiennes ont saisi un navire battant pavillon asiatique à destination du Pakistan. Lors d'une enquête, les autorités indiennes ont confirmé que les documents comportaient une fausse déclaration concernant les articles à double usage de la cargaison. Les enquêteurs indiens ont certifié que les articles expédiés étaient des « autoclaves », utilisés pour les matériaux sensibles à haute énergie et pour l'isolation et le revêtement chimique des moteurs de missiles. Ces articles sensibles figurent sur les listes de contrôle des exportations de biens à double usage du Régime de contrôle des technologies des missiles de l'Inde et d'autres juridictions.56

Le connaissement de la cargaison saisie a fourni la preuve du lien entre l'importateur et le Complexe national de développement, qui est impliqué dans le développement de missiles balistiques à longue portée.

Source : Inde

56 L'exportation de tels équipements sans l'approbation formelle de diverses autorités constitue une violation de la loi en vigueur. et des alliances.

5. Section 3. Défis et bonnes pratiques en matière d'atténuation des risques liés au PF

Détection par le biais de SAR/STR et de contrôles des sanctions

96. Pour détecter les méthodes d'évasion fiscale et de contournement des sanctions, les pays s'appuient largement sur les rapports d'enquête et de signalement (SAR) Les obligations et les contrôles rigoureux des sanctions correspondent. Pour compléter ces techniques et identifier et combattre efficacement les activités illicites à l'échelle mondiale, d'autres méthodes de détection incluent le partage de renseignements transfrontaliers, la coordination interinstitutionnelle, la coopération internationale et des outils de surveillance, notamment les renseignements de sources ouvertes et l'analyse de la blockchain.

97. De nombreux pays ont indiqué s'appuyer sur des obligations rigoureuses en matière de déclarations d'infractions et de déclarations de soupçons (SAR/STR) pour détecter les stratagèmes de fraude fiscale et de contournement des sanctions, afin d'identifier et de combattre des tactiques complexes et évolutives. La diversité des cadres juridiques nationaux et des obligations de déclaration peut obliger les entités déclarantes à soumettre des SAR/STR concernant, plus généralement, le fraude fiscale et le contournement des sanctions. Plusieurs pays soulignent que les obligations des entités déclarantes peuvent inclure la mise en œuvre d'une diligence raisonnable rigoureuse à l'égard de la clientèle, le respect des dispositions législatives et réglementaires, la surveillance des transactions impliquant des pays à haut risque et le respect de toutes les obligations en matière de SAR/STR lorsque des transactions suspectes sont identifiées.

Bonnes pratiques pour détecter les fraudes financières et les évasions de sanctions par le biais de SAR/STR et Contrôle des sanctions

98. En outre, plusieurs pays exigent des entités déclarantes qu'elles intègrent des systèmes automatisés de filtrage des sanctions à leurs obligations, notamment en ce qui concerne leurs politiques et procédures internes, afin d'améliorer l'efficacité des SAR/STR. Les listes de sanctions internationales et/ou nationales sont intégrées aux systèmes de filtrage des sanctions, ce qui permet aux entités déclarantes de trouver des correspondances avec des personnes ou des entités et d'utiliser des mots-clés relatifs aux transactions à haut risque et aux personnes, entités ou activités sanctionnées. Dans certains pays, une correspondance positive trouvée lors du filtrage peut entraîner des obligations supplémentaires pour les entités déclarantes : soumettre des SAR/STR et informer les autorités des avoirs gelés sous sanctions ou des transactions liées à des entités sanctionnées. Les deux études de cas ci-dessous illustrent le fonctionnement des SAR/STR.
ont été utilisés pour lancer des enquêtes.

Encadré 35. Étude de cas : Le filtrage des informations négatives et les rapports d'enquête et de soupçon (SAR/STR) permettent de détecter les achats illicites de biens à double usage.

Deux sociétés françaises ont servi d'intermédiaires pour l'achat de composants électroniques à double usage d'origine américaine, qui ont été revendus par l'intermédiaire d'une série d'entités à un groupe américain. entreprise sanctionnée en Russie.

L'affaire a été détectée par les autorités françaises, en collaboration avec le secteur privé, grâce à la surveillance des informations négatives concernant la Russie et des SAR/STR des banques, suite à l'émission par TracFin d'un « appel à la vigilance » visant une personne et des entités concernées (l'UBO des entités). La publication de TracFin a également pointé du doigt l'épouse de l'individu, nommée directrice de l'une des entités moins d'un mois avant que son mari ne soit désigné comme SDN par l'OFAC.

L'enquête a nécessité une coopération interinstitutionnelle étroite et un partenariat fructueux avec les institutions financières, y compris un suivi régulier avec les banques concernées pour éviter toute fuite de capitaux et garantir que les fonds existants n'étaient effectivement pas disponibles pendant l'enquête.

Source : France

99. Plusieurs pays ont investi dans la formation, la sensibilisation, les orientations spécialisées et les mécanismes de surveillance par le biais de partenariats public-privé afin de renforcer la conformité et d'améliorer les capacités de détection. À cette fin, la publication d'avis, d'orientations ou d'indicateurs nationaux ou internationaux peut aider les entités déclarantes à détecter les cas présumés de contournement des sanctions et d'activités de financement du terrorisme et à soumettre des rapports d'alerte (SAR) et des déclarations de soupçon spécifiques afin de respecter leurs obligations. Certains pays ont également adopté des cadres juridiques nationaux obligeant les entités réglementées à déposer des SAR et des déclarations de soupçon (SAR) sur la base de ces avis ou alertes, renforçant ainsi leurs capacités de détection.

Encadré 36. Étude de cas : Émission d'alertes détaillées pour faciliter le dépôt des SAR/STR par les institutions financières

Afin de faciliter le dépôt par les institutions financières de déclarations d'infractions (SAR) et de déclarations de soupçon (STR) relatives à l'évasion fiscale américaine liée à la Russie et à la Biélorussie, le BIS et le FinCEN ont publié une alerte conjointe en 2022. Cette alerte leur a fourni un aperçu des restrictions d'exportation actuelles du BIS ; une liste des produits susceptibles d'être sous-estimés ; et une sélection d'indicateurs transactionnels et comportementaux pour les aider à identifier les transactions suspectes liées à une possible évasion fiscale. L'alerte demandait également aux institutions financières d'utiliser le terme clé « FIN-2022-RUSSIABIS » lors du dépôt de déclarations d'infractions (SAR) et de déclarations de soupçon (STR).

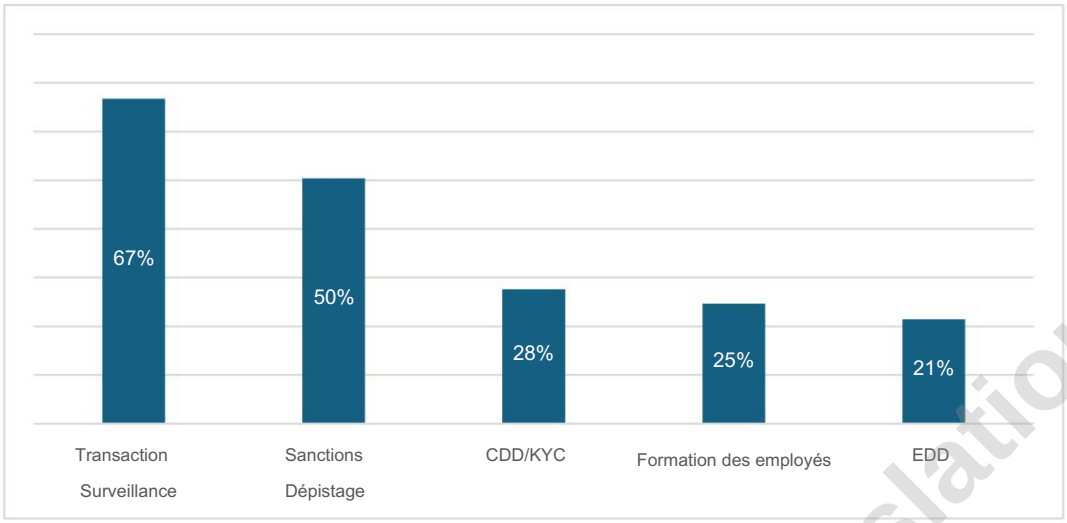
Dans le prolongement de cette alerte, le BIS et le FinCEN ont publié une alerte conjointe en novembre 2023, mettant en évidence les signaux d'alerte liés à l'évasion mondiale des contrôles à l'exportation. Cette alerte demandait aux institutions financières d'utiliser le terme clé « FIN-2023-GLOBALEXPORT » lors du dépôt de leurs déclarations de soupçons et de déclarations de soupçons. Les institutions financières ont soumis davantage de déclarations de soupçon et de déclarations de soupçons avec le terme clé relatif à la Russie qu'avec le terme clé relatif aux exportations mondiales, principalement parce que les restrictions à l'exportation imposées à la Russie et à la Biélorussie sont plus larges et permettent aux institutions financières d'identifier plus facilement les transactions financières potentiellement liées dans les informations qu'elles reçoivent.

Source : États-Unis

100. Selon la plupart des entités du secteur privé qui ont répondu à la consultation publique du GAFI, les meilleurs moyens d'atténuer les risques liés à l'évasion des sanctions et au PF sont liés à des mesures préventives clés de LBC/FT telles que la diligence raisonnable à l'égard de la clientèle, l'évaluation complète des risques, les outils de filtrage des sanctions et la surveillance continue qui peuvent conduire à la

Dépôt de déclarations de soupçon et de soupçon, formation des employés, politiques et procédures, filtrage des informations négatives et diligence raisonnable renforcée (voir la figure 3 pour les bonnes pratiques les plus citées par le secteur privé). De plus, les mesures de prévention du blanchiment d'argent par le biais du commerce, les alertes en temps réel et les solutions technologiques avancées ont été citées comme importantes. Cependant, en l'absence de mécanismes solides de partage d'informations, il peut être difficile pour le secteur privé de détecter les schémas complexes de fraude fiscale et de contournement des sanctions par le biais de processus standard de gestion des risques.

Figure 3. Bonnes pratiques pour détecter le contournement des sanctions



Défis liés à la détection des fraudes financières et des évasions de sanctions par le biais des SAR/STR et Contrôle des sanctions

101. Près d'un tiers des pays n'ont pas signalé l'utilisation des DAS/DOS comme méthode de détection du PF. Le fait qu'un nombre important de pays ne criminalisent pas le PF peut expliquer pourquoi certains pays n'y ont pas recours dans une certaine mesure. Les pays qui ne considèrent pas le PF comme une infraction pénale sont peut-être moins susceptibles d'exiger des entités déclarantes qu'elles identifient le PF dans les DAS/DOS. De leur côté, les entités déclarantes peuvent déposer des DAS/DOS impliquant des acteurs du PF, mais les informations essentielles les reliant aux activités du PF peuvent être absentes sans davantage d'indications sur la complexité de la détection de cette activité illicite.

102. Par ailleurs, l'intégration des listes de sanctions dans les cadres nationaux de rapports d'enquête et de déclarations de soupçons (SAR/STR) et l'utilisation d'outils de filtrage peuvent jouer un rôle central dans la détection des soupçons de fraude fiscale et de contournement des sanctions. Certains pays ont constaté des difficultés avec les correspondances de filtrage des sanctions, car ils ont constaté des correspondances faussement positives avec des personnes/entités ou des informations non pertinentes suite à des recherches par mots-clés génériques. De plus, la nécessité de comparer plusieurs identifiants, notamment les dates de naissance, les noms, les pseudonymes, les versions multiples des noms, les différences phonétiques et orthographiques des noms et les numéros de passeport, rend les algorithmes de correspondance plus susceptibles de détecter des faux positifs. Cependant, des mesures d'atténuation peuvent inclure la détection de faux positifs, l'utilisation de renseignements de sources ouvertes tels que les registres des sociétés ou les BOI, et la corroboration des informations avec d'autres bases de données.

103. Les pays ont signalé un autre défi concernant le faible niveau de compréhension et de respect des obligations en matière de PF parmi les entreprises et professionnels non financiers désignés (EPNFD). Nombre d'entre elles ignorent leurs responsabilités en matière de surveillance et de déclaration des activités liées aux PF. 57 Dans certains pays, cela peut rendre difficile pour les autorités de détecter les activités de PF dans des secteurs autres que les institutions financières.

Toutefois, les entités du secteur privé de tous les secteurs ont signalé un manque de retour d'information du secteur public sur des SAR/STR pertinents, ce qui peut rendre plus difficile la résolution de ce défi.

57 Voir la section deux, Atténuation des risques liés aux PF, dans les Orientations du GAFI sur les PF de 2021 pour plus d'informations sur les mesures d'atténuation des risques prises par les institutions financières, les entreprises et professions non financières désignées et les prestataires de services d'investissement VASP.

Autres méthodes de détection

104. En complément des SAR/STR et des vérifications des sanctions, d'autres méthodes de détection comprennent le renseignement transfrontalier, le partage d'informations grâce à la coordination interinstitutions et à la coopération internationale, ainsi que les outils de surveillance. Il est important de noter que les pays intègrent souvent plusieurs sources de détection pour obtenir une vision globale des schémas de financement illicite et d'évasion fiscale.

105. De nombreux pays signalent que les autorités douanières et le renseignement transfrontalier jouent un rôle essentiel dans la détection et les enquêtes sur les activités liées au PF, en particulier les liens avec les pays et les routes commerciales à haut risque. Les services douaniers collaborent avec les organismes régionaux et internationaux et peuvent échanger des informations sur les enquêtes, les déclarations douanières, les données d'importation/exportation et les demandes de licences afin d'améliorer la détection et les enquêtes sur les violations potentielles liées au contournement des sanctions par les bailleurs de fonds de la prolifération.
Cet échange améliore les capacités de détection et aide à enquêter sur les violations potentielles.
En particulier, les activités clés dans ce domaine comprennent l'analyse et le suivi des opérations de commerce extérieur et des mouvements de marchandises, y compris les flux d'actifs vers les pays à haut risque, les matériels de défense et les biens stratégiques et à double usage. Le partage de renseignements, associé à des cadres réglementaires juridictionnels pour garantir la conformité, souligne le rôle crucial des autorités douanières dans la détection des violations potentielles liées au PF et au contournement des sanctions.

Bonnes pratiques pour détecter les fraudes financières et l'évasion des sanctions par d'autres moyens de détection Mesures

Coordination interinstitutions

106. La plupart des pays ont souligné l'importance de la coordination interinstitutionnelle pour détecter les cas de fraude fiscale et de contournement des sanctions. Plus précisément, les enquêtes des services répressifs et les échanges d'informations avec d'autres autorités compétentes peuvent donner lieu à des saisines des services nationaux, à des enquêtes conjointes et à des actions de sensibilisation, ce qui peut contribuer à identifier les flux financiers de fonds et/ou d'actifs des personnes et entités désignées. La collecte de renseignements, complétée par des travaux d'enquête, constitue une approche multidisciplinaire pour identifier et détecter les cas suspects de fraude fiscale et de contournement des sanctions.

Encadré 37. Étude de cas : Coordination interinstitutions sur l'exportation de biens à double usage contrôlés

En 2017, le CANAFE a reçu des renseignements volontaires des organismes canadiens d'application de la loi indiquant qu'une entreprise canadienne d'électronique était soupçonnée d'être impliquée dans l'expédition de circuits intégrés à double usage contrôlés.

Les rapports SAR/STR indiquaient que l'activité transactionnelle de la société correspondait à certains des principaux critères caractéristiques des systèmes de blanchisseries russes et est-européennes. Un rapport SAR/STR indiquait :

- Les fonds proviennent de personnes de haut rang ;
- Les personnes situées dans des pays comme la Russie, l'Azerbaïdjan, ainsi que d'autres pays d'Europe de l'Est;
- Des individus de haut rang ont ouvert des sociétés écrans dans le but de blanchir des fonds ;

• Sociétés écrans enregistrées dans des paradis fiscaux ; • Fonds transférés via des sociétés écrans dans des paradis fiscaux. • La société a reçu des virements électroniques de fonds provenant de pays potentiellement intermédiaires pour le transbordement de biens à double usage ou d'autres activités financières illicites (y compris plusieurs pays européens). Dans certains cas, le pays d'origine ne correspondait pas à l'adresse indiquée pour les entités chargées de commander les virements électroniques. De plus, la société était bénéficiaire de virements électroniques de fonds commandés par des personnes et des entités dont les adresses étaient répertoriées en Russie.

Le SAR/STR a noté que les fonds de la société ont été épuisés par de multiples chèques envoyés aux actionnaires et par des transferts électroniques de fonds vers une société de traitement des paiements en ligne.

Interrogés sur l'impact des divulgations de renseignements du CANAFE concernant l'entreprise, les organismes canadiens d'application de la loi ont indiqué que ces renseignements avaient déclenché une nouvelle enquête et leur avaient fourni des informations supplémentaires et inconnues. Ils ont précisé que les divulgations et la collaboration du CANAFE avaient été des facteurs clés dans leur compréhension des réseaux impliqués et dans le succès global de leurs enquêtes. Ils ont ajouté que les renseignements fournis par le CANAFE avaient contribué à la recherche d'actes d'accusation officiels dans un pays partenaire.

Source : Canada

107. En outre, certains pays ont souligné que la publication de documents d'orientation, qui peuvent inclure des tendances, des typologies et des indicateurs, est essentielle pour détecter les activités suspectes (voir la section sur la coordination et la collaboration nationales).

Coopération internationale

108. Compte tenu de la dimension mondiale du PF et du contournement des sanctions, la coopération internationale par le biais du renseignement et du partage d'informations constitue un instrument majeur de détection et de prévention. Des mesures de détection efficaces nécessitent une approche coordonnée entre les autorités nationales et les partenaires internationaux. Par exemple, les CRF peuvent favoriser le partage d'informations par l'intermédiaire du Groupe Egmont, qui joue un rôle essentiel en facilitant le partage d'informations entre les CRF, améliorant ainsi la détection des activités financières suspectes liées au PF.

ou des sanctions. En outre, la coopération internationale peut aider les pays à analyser systématiquement les risques associés au mouvement du commerce international, ce qui peut contribuer à renforcer les profils de risque nationaux.

Outils de surveillance

109. Les outils de surveillance jouent également un rôle important dans la détection des fraudes financières et du contournement des sanctions. Ces outils exploitent diverses sources de données, notamment des renseignements en libre accès et des techniques sophistiquées d'analyse de la blockchain. Les autorités compétentes peuvent utiliser ces renseignements pour accéder à un large éventail d'informations, notamment des registres d'entreprises, des informations sur la propriété effective, des images satellite et des données géospatiales, qui peuvent révéler des réseaux d'acteurs illicites.

110. Plusieurs pays ont également indiqué que les outils d'analyse de la blockchain aident à détecter le contournement des sanctions et les activités de financement public. L'utilisation d'actifs virtuels peut complexifier la détection, mais les transactions sur des actifs virtuels fonctionnant sur des blockchains publiques peuvent être tracées. L'analyse de la blockchain permet aux autorités compétentes de surveiller et de tracer les flux de fonds, d'identifier les activités suspectes et d'atténuer certaines tentatives d'obscurcissement des actifs virtuels.
Pour plus d'informations, veuillez consulter la typologie 3 (Utilisation d'actifs virtuels et d'autres technologies).

Défis liés à la détection des fraudes financières et des évasions de sanctions par d'autres moyens de détection

Mesures

111. Les pays ont signalé plusieurs difficultés de détection, notamment les différences de juridiction dans les programmes de sanctions et les divergences qui en découlent entre les listes d'entités sanctionnées, les exigences juridiques nationales et les diverses réglementations d'application. Un autre défi majeur réside dans le recours par la RPDC à du personnel diplomatique pour faciliter la fourniture de services financiers ou le transfert d'actifs ou de ressources sanctionnés, notamment le transport d'espèces en vrac. La RPDC recourt à l'immunité diplomatique pour échapper aux contrôles et aux enquêtes. De nombreux pays s'inquiètent du manque de cohérence dans la collecte et/ou la disponibilité des informations sur les bénéficiaires effectifs, ce qui complique encore la détection des fraudes financières et du contournement des sanctions (voir la typologie 2 et la section « Vulnérabilités » pour plus d'informations).

Enquête et poursuites

112. Depuis la publication du rapport du GAFI Combattre le PF : Rapport de situation sur l'élaboration des politiques et la consultation en 201058, les cadres juridiques visant à prévenir et à combattre le PF et l'évasion des sanctions ont peut-être été considérablement renforcés, mais les exemples d'enquêtes et de poursuites efficaces restent rares en 2025. Comme décrit dans le rapport du GAFI de 2010, la difficulté de poursuivre les affaires de PF a été attribuée à plusieurs défis, notamment : la non-criminalisation du PF ; la collecte de preuves dans les affaires de PF ; la nature internationale des activités de PF ; le recours à des intermédiaires financiers pour masquer des activités illicites ; des cadres inefficaces pour le contrôle des exportations ; l'absence d'une définition universellement acceptée des ADM PF ; et les différences dans les approches juridictionnelles du sujet, y compris la coopération internationale.

D'après les contributions du Réseau mondial du GAFI, bon nombre des mêmes défis fondamentaux semblent encore constituer des obstacles à la réussite des enquêtes et des poursuites dans les affaires complexes de PF (et d'évasion des sanctions).

58 LUTTE CONTRE LE FINANCEMENT DE LA PROLIFÉRATION

Techniques et mécanismes d'enquête

Bonnes pratiques en matière d'enquêtes PF

113. De nombreux pays ont indiqué que l'efficacité des enquêtes sur les fraudes financières et le contournement des sanctions repose sur l'application de procédures normalisées pour les affaires de criminalité financière et sur une collaboration entre les partenaires interinstitutions concernés. Les rapports d'enquête et de déclaration de soupçons (SAR) sont essentiels pour identifier et comprendre les tendances inhabituelles des activités financières. Leur utilisation permet également de révéler les liens entre les entreprises et les individus impliqués dans le contournement des sanctions et les activités illicites.

114. Certains pays ont indiqué qu'un autre outil d'enquête important est le suivi des actifs virtuels, parfois utilisés pour échapper à la détection. Les enquêteurs peuvent suivre l'argent grâce à l'analyse de la blockchain, même pour les petits montants, et découvrir ainsi des schémas financiers et des liens avec les entités et les individus concernés.

115. L'analyse avancée joue un rôle important dans la lutte contre le financement du terrorisme en identifiant des tendances et des activités inhabituelles dans les données financières. Ces outils peuvent aider les enquêteurs à découvrir des liens entre des entités et à identifier des réseaux de personnes ou d'entreprises impliqués dans le contournement des sanctions. Par exemple, l'analyse avancée permet l'analyse des liens, qui relie les comptes, les transactions et les parties prenantes afin de mettre en évidence le fonctionnement des réseaux illégaux. Les outils de surveillance en temps réel permettent aux autorités d'agir rapidement en cas d'activités suspectes.
La combinaison de données provenant de différentes sources, telles que les institutions financières, les registres douaniers et les rapports de renseignement, améliore également l'efficacité et la complétude des enquêtes. Ces outils permettent d'identifier des schémas de transactions inhabituels ou de détecter l'utilisation de technologies de protection de la vie privée pour dissimuler l'origine des fonds. Le partage de ces informations entre les agences renforce l'efficacité de ces outils dans la lutte contre le financement du terrorisme.

116. Quelques pays ont indiqué qu'il était important d'envisager les mêmes tactiques que celles utilisées dans les enquêtes sur les trafiquants de drogue et les escrocs, comme le recours à des agents infiltrés et à des sources confidentielles.

Encadré 38. Étude de cas : Utilisation d'agents infiltrés et de sources confidentielles contre un trafiquant de matières nucléaires

Le 21 février 2024, le ministère de la Justice des États-Unis (DOJ) et la Drug Enforcement Administration (DEA) des États-Unis ont annoncé la publication d'un acte d'accusation de remplacement accusant un accusé de complot avec un réseau d'associés en vue de faire transiter des matières nucléaires du Myanmar vers d'autres pays. Au cours de ce complot, l'accusé et ses complices ont montré des échantillons de matières nucléaires en Thaïlande à un agent infiltré de la DEA (« UC-1 »), qui se faisait passer pour un trafiquant de stupéfiants et d'armes. Avec l'aide des autorités thaïlandaises, les échantillons nucléaires ont été saisis puis transférés aux forces de l'ordre américaines. Un laboratoire de criminalistique nucléaire américain a ensuite analysé les échantillons et confirmé leur présence d'uranium et de plutonium de qualité militaire.

Le défendeur et son coaccusé avaient déjà été inculpés en avril 2022 de trafic international de stupéfiants et d'infractions liées aux armes à feu, et tous deux avaient été placés en détention.

Selon les allégations contenues dans l'acte d'accusation de remplacement, début 2020, l'accusé a informé UC-1 et une source confidentielle de la DEA (« CS-1 ») qu'il avait accès à une grande quantité de matières nucléaires qu'il souhaitait vendre. Plus tard dans l'année, l'accusé a envoyé à UC-1 une série de photographies représentant des substances rocheuses avec des compteurs Geiger mesurant les radiations, ainsi que des pages de ce qu'il a présenté comme des analyses de laboratoire indiquant la présence de thorium et d'uranium dans les substances représentées.
En réponse aux demandes répétées du défendeur, UC-1 a accepté, dans le cadre de l'enquête de la DEA, d'aider ce dernier à négocier la vente de ses matières nucléaires à son associé, qui se faisait passer pour un général iranien (le « Général »), en vue de leur utilisation dans un programme d'armement nucléaire. Le défendeur a ensuite proposé au Général de lui fournir du « plutonium », encore plus « performant » et « puissant » que l'uranium à cette fin.

Lors de leurs discussions concernant l'accès du défendeur aux matières nucléaires, ce dernier a également discuté avec UC-1 de son désir d'acheter des armes de qualité militaire. À cette fin, en mai 2021, le défendeur a envoyé à UC-1 une liste d'armes, dont des missiles sol-air, qu'il souhaitait acheter auprès d'UC-1 pour le compte du chef d'un groupe ethnique insurgé au Myanmar (« CC-1 »). Avec deux autres co-conspirateurs (« CC-2 » et « CC-3 »), le défendeur a proposé à UC-1 que CC-1 vende de l'uranium à la

Général, par l'intermédiaire du défendeur, pour financer l'achat d'armes de CC-1.

Le 8 janvier 2025, l'accusé a plaidé coupable de complot en vue de trafic de matières nucléaires, notamment d'uranium et de plutonium de qualité militaire, du Myanmar vers d'autres pays, ainsi que de trafic international de stupéfiants et d'armes.

Source : États-Unis

117. Enfin, de nombreux pays ont souligné l'importance de la coopération interinstitutionnelle par le biais de réunions régulières, notamment par la création de groupes de travail spécialisés et d'experts. La collaboration entre les institutions financières, les autorités douanières et les services répressifs peut améliorer les enquêtes et aboutir proactivement au gel des avoirs et à l'interception des envois liés au financement du terrorisme et au contournement des sanctions.

Encadré 39. Exemples de juridiction : Groupes de travail et groupes d'intervention spécialisés pour lutter contre le PF et l'évasion des sanctions

- France : Un groupe de travail spécialisé, dirigé par TracFin (la cellule de renseignement financier), a enquêté sur deux sociétés (entités A1 et A2) fournissant des composants électroniques à une entité russe sanctionnée. Ces sociétés ont agi comme intermédiaires, achetant les composants et les transférant à des groupes sanctionnés par l'intermédiaire d'une autre société dans un pays tiers. Le groupe de travail comprenait TracFin, des institutions financières et des forces de l'ordre. Ils ont analysé les déclarations d'infraction et de soupçon soumises par les banques, surveillé les flux financiers des sociétés et suivi l'implication des bénéficiaires effectifs. Leurs efforts coordonnés ont abouti au gel des avoirs des sociétés et à l'arrêt de leurs activités.

- Indonésie : Un groupe de travail a enquêté sur un vraquier, le Petrel 8, impliqué dans le transport de charbon vers la RPDC en violation des sanctions de l'ONU. Ce groupe de travail comprenait le ministère des Affaires étrangères, les autorités douanières et la Cellule de renseignement financier (PPATK). Ils ont combiné les renseignements financiers et les registres d'expédition pour établir que le navire appartenait à une société indonésienne et avait déjà été sanctionné pour des activités similaires. Le groupe de travail a coordonné ses activités avec le Comité des sanctions de l'ONU, ce qui a conduit à l'immobilisation du navire et à son démantèlement.

Sources : France et Indonésie

Défis dans la poursuite de l'enquête PF

118. En général, les enquêtes sur le blanchiment d'argent (BA) et le financement du terrorisme (FT) diffèrent à bien des égards des enquêtes sur le blanchiment d'argent (BA) et le financement du terrorisme (FT). Le FT se concentre sur les activités de financement qui contribuent à soutenir les programmes d'armes de destruction massive. Il implique souvent de puissants acteurs étatiques ou des groupes utilisant des sociétés écrans, des échanges commerciaux et des structures de propriété complexes pour échapper aux sanctions. Contrairement au BA, qui dissimule l'origine des capitaux illégaux, et au FT, qui finance le terrorisme, les enquêtes sur le FT s'appuient davantage sur des renseignements relatifs à d'éventuelles violations des contrôles à l'exportation et des sanctions. Le FT peut être plus difficile à enquêter car les risques qu'il comporte sont moins connus et il implique souvent l'utilisation de biens légaux (y compris des biens contrôlés) à des fins illégales.
Les enquêteurs ont besoin d'une coopération nationale et internationale plus forte et d'outils d'analyse avancés pour résoudre les affaires de PF, qui peuvent être plus complexes que ce qui est nécessaire régulièrement dans les affaires de BC ou de FT.

119. De nombreux pays ont signalé des difficultés similaires, notamment des systèmes de financement par capitaux propres utilisant des sociétés écrans, des niveaux de propriété multiples et des transactions de faible ampleur, mais fréquentes. Ces tactiques compliquent considérablement la tâche des acteurs concernés, notamment les services répressifs, les régulateurs, les institutions financières, les CRF et les procureurs, qui s'appuient sur des données précises et une collaboration étroite pour retrouver les bénéficiaires effectifs ou les organisations impliquées dans des systèmes complexes (voir typologie 2).

120. Un autre défi réside dans le manque de sensibilisation aux risques, aux tendances et aux méthodes du PF au sein des institutions financières et autres entités réglementées, notamment l'insuffisance de la formation sur les risques du PF pour améliorer la qualité des rapports d'analyse et de déclaration de soupçons (SAR) et des déclarations de soupçons (STR). Comme indiqué dans la section précédente du présent rapport, de nombreux pays ne criminalisent pas le PF. Cela peut expliquer en partie les lacunes liées au nombre et à la qualité des SAR et des déclarations de soupçons pertinents.

121. Plus généralement, les ressources limitées des autorités gouvernementales et des entités du secteur privé constituent également un défi pour de nombreux pays. Les petits pays, en particulier, peuvent manquer de financement ou d'expertise pour traiter des affaires complexes. Cela pourrait également constituer un défi de priorisation qui se répercute sur l'allocation des ressources dans les secteurs public et privé. Si certains pays ont établi une infraction principale incluant le PF ou ont recours à des infractions accessoires pour poursuivre les actes de PF, l'absence d'approche cohérente en matière de criminalisation peut perturber la coopération internationale en matière d'enquêtes et de poursuites dans les affaires liées au PF.

122. Enfin, les affaires transfrontalières nécessitent une coopération avec d'autres pays, mais les différences entre les systèmes juridiques, telles que les règles d'admissibilité des preuves, les définitions variables des délits financiers et l'absence de double incrimination, compliquent la conduite des enquêtes transfrontalières. En l'absence d'accords entre les pays,
pour partager des informations, il peut y avoir des retards importants ou des demandes d'informations rejetées pour les enquêtes (voir la section Coopération internationale).

Poursuites et autres méthodes

Bonnes pratiques en matière de poursuites pénales

123. De nombreux pays ont indiqué que poursuivre les affaires complexes de fraude fiscale et de contournement des sanctions est encore plus compliqué que d'enquêter sur celles-ci. Le succès des poursuites dans ces affaires nécessite un cadre juridique solide, notamment des lois claires définissant la fraude fiscale et ses activités connexes, ainsi que la capacité de recueillir et de présenter des preuves devant les tribunaux.

124. La coordination des efforts entre les unités d'enquête et les procureurs est également essentielle pour constituer des dossiers solides. S'inspirer des précédents et connaître les typologies et les nouvelles méthodes utilisées par les auteurs de fraudes au PF et de fraudes aux sanctions peut améliorer les chances de succès des enquêtes et, par conséquent, des poursuites. De plus, les partenariats mondiaux peuvent jouer un rôle important dans les poursuites contre les auteurs de fraudes au PF, soulignant l'importance de la coopération internationale pour lutter contre ces crimes complexes. Enfin, des réglementations strictes en matière de confiscation et de recouvrement d'avoirs pourraient entraîner davantage de poursuites, notamment pour les fonds sortant du pays.

Défis dans la poursuite des affaires de PF

125. La plupart des pays ont indiqué que la poursuite des affaires complexes de fraude fiscale et de contournement des sanctions est difficile. Certains pays ont évoqué des difficultés de preuve pour prouver que des marchandises contrôlées ou interdites ont été envoyées vers une juridiction sanctionnée. Lorsque ces difficultés de preuve sont insurmontables, il existe des exemples de procureurs poursuivant les contrevenants pour d'autres infractions commises afin de dissimuler leur infraction de fraude fiscale, telles que l'entrave à la justice ou la falsification. D'autres ont mentionné que l'immunité diplomatique peut limiter la poursuite de certaines affaires de fraude fiscale ou de contournement des sanctions.

126. Un autre défi auquel sont confrontés les pays est de prouver que les activités financières sont directement liées au financement du terrorisme ou au contournement des sanctions, en particulier lorsque les preuves sont dispersées dans différents pays. Cela nécessite une documentation détaillée et une coopération internationale étroite, ce qui n'est pas toujours facile à mettre en œuvre dans des dossiers aussi complexes.

127. Le partage d'informations et de renseignements entre les pays peut contribuer à combler les lacunes en matière de répression, et les pays peuvent ainsi traiter plus efficacement les affaires transfrontalières et empêcher les réseaux de FP d'exploiter les faiblesses du système financier mondial. Cependant, de nombreux pays ne disposent pas de ces mécanismes.

128. La formation et la sensibilisation sont également essentielles à la réussite des poursuites, même si de nombreuses institutions financières, entreprises et même procureurs manquent de compréhension des risques et de la complexité du PF. Une formation adéquate peut les aider à reconnaître les activités suspectes et à comprendre le fonctionnement des systèmes de PF. Ceci est particulièrement important dans les pays disposant de ressources ou d'une expertise limitées dans le traitement des affaires de PF.

Autres mesures visant à dissuader les contrevenants aux sanctions

129. Comme indiqué dans cette section, les autorités gouvernementales peuvent envisager des poursuites pénales en cas de violation des TFS. De plus, certains pays envisagent d'autres options répressives pour remédier aux violations des TFS, notamment en matière de PF. Étant donné que de nombreux pays
Même si les États semblent être confrontés à des défis notables dans la poursuite des affaires complexes de fraude fiscale et de contournement des sanctions, il peut être utile d'envisager d'autres mesures dans les circonstances appropriées.

Encadré 40. Exemples de juridiction : Mesures d'exécution civiles et pénales en complément ou en alternative aux poursuites pénales

• Commission européenne : La directive 2024/1226 de l'UE du 24 avril 2024 a introduit de nouvelles règles visant à établir des normes de base communes pour les sanctions pénales pour les personnes physiques et les sanctions pénales ou non pénales pour les personnes morales dans tous les États membres, comblant ainsi les lacunes juridiques existantes et renforçant l'effet dissuasif de la violation des sanctions de l'UE en premier lieu.59

Royaume - Uni : Toute violation des sanctions financières peut constituer une infraction pénale, passible d'une peine d'emprisonnement pouvant aller jusqu'à sept ans. Il existe des sanctions civiles et pénales pour remédier aux violations des sanctions financières. Les forces de l'ordre peuvent envisager des poursuites pour violation des sanctions financières. Le régime de sanctions pécuniaires créé par la loi de 2017 offre une alternative aux poursuites pénales pour les violations de la législation sur les sanctions financières. L'OFSI est la branche du Trésor de Sa Majesté qui impose ces sanctions pécuniaires.60

États -Unis : Les pouvoirs d'enquête et d'application de l'OFAC sont exclusivement de nature civile, contrairement aux pouvoirs d'application des sanctions pénales exercés par le DOJ, le DHS et le Department of Commerce dans ce domaine. Le cas échéant, les mesures d'application soulignent l'importance de programmes de conformité aux sanctions solides et efficaces, en particulier pour les entreprises impliquées dans des transactions internationales complexes, afin de garantir la mise en place de mesures visant à prévenir toute implication dans des stratagèmes d'évasion des sanctions.

• En avril 2023, British American Tobacco (BAT), fabricant de tabac et de cigarettes, a accepté de payer 508 612 492 dollars pour régler sa responsabilité civile potentielle pour violations apparentes des sanctions de l'OFAC contre la RPDC et les prolifératurs d'armes de destruction massive. En exportant du tabac et des produits connexes et en recevant le paiement de ces exportations, BAT a incité des institutions financières américaines à traiter des virements électroniques contenant les droits de propriété bloqués de banques nord-coréennes sanctionnées, à exporter des services financiers et à faciliter l'exportation de tabac vers la RPDC.61

En avril 2022, l'OFAC a conclu un accord transactionnel avec Toll Holdings Limited (« Toll »), une société internationale de transport de fret et de logistique basée en Australie, pour violations apparentes de plusieurs programmes de sanctions, notamment le traitement de transactions impliquant la RPDC, l'Iran et la Syrie. L'une des principales vulnérabilités résidait dans l'absence de gestion des risques et de diligence raisonnable au sein de la fonction conformité de Toll.62

Sources : Commission européenne, Royaume-Uni et États-Unis

Coordination et collaboration nationales

Mécanismes interinstitutions

130. Un cadre interinstitutionnel efficace contribue à atténuer les risques liés aux stratagèmes complexes de fraude fiscale et de contournement des sanctions. Pour développer des cadres interinstitutionnels efficaces,

Les pays soulignent la nécessité d'une coopération et d'une coordination continues entre les autorités gouvernementales compétentes. Pour de nombreux pays, les acteurs concernés comprennent les responsables de la LBC/FT/CPF, les services répressifs, les superviseurs, le pouvoir judiciaire, les autorités de contrôle et d'octroi de licences à l'importation et à l'exportation, les douanes, les services de contrôle aux frontières et les services de renseignement. Les pays signalent qu'une coopération et une coordination étroites entre nombre de ces autorités compétentes facilitent l'échange d'informations pertinentes et opportunes. Grâce à ce processus interinstitutionnel, les autorités gouvernementales sont les mieux placées pour contribuer à l'ouverture et à la poursuite d'enquêtes sur d'éventuelles violations du régime TFS et d'autres activités de PF pertinentes.

Bonnes pratiques pour la coopération interinstitutions

131. Sur la base des contributions présentées dans l'ensemble du réseau mondial du GAFI, les pays utilisent des mécanismes interinstitutions pour lutter contre le PF et l'évasion des sanctions dans l'une des trois catégories qui se chevauchent : 1) coordination générale sur les opérations financières transfrontières, qui comprend le PF-PF ; 2) une attention particulière portée aux PF-PF et aux réglementations sur les contrôles des exportations ; ou 3) une attention particulière portée aux PF-PF et aux réglementations sur les contrôles des exportations, ainsi qu'un champ de coordination plus large pour lancer des enquêtes, des poursuites et d'autres mesures complexes en matière de PF et d'évasion des sanctions.

132. En vertu de la recommandation 7 du GAFI, le réseau mondial du GAFI est tenu de mettre en œuvre le TFS sans délai afin de se conformer à toutes les résolutions du Conseil de sécurité des Nations Unies relatives au PF.63 La plupart des pays Vérification de l'établissement d'un cadre juridique pour la mise en œuvre du PF-TFS, qui implique souvent le recours aux mécanismes interinstitutionnels existants en matière de TFS. Ce type de mécanisme interinstitutionnel permet aux pays de satisfaire à leurs exigences minimales fondées sur des règles pour faire face aux violations, non-applications ou contournements potentiels des TFS mentionnés dans la recommandation 7.

59 Les nouvelles règles visent à garantir que de telles violations puissent faire l'objet d'enquêtes et de poursuites pénales dans tous les États membres. Elles comprennent une liste d'infractions pénales liées à la violation et au contournement des sanctions de l'UE, telles que : le défaut de gel des avoirs ; la violation des interdictions de voyager et des embargos sur les armes ; la fourniture de services économiques et financiers interdits ou restreints, le transfert de fonds qui devraient être gelés à un tiers ou la fourniture de fausses informations pour dissimuler des fonds qui devraient être gelés. Elles comprennent également des règles renforcées sur le gel et la confiscation des produits, instruments et avoirs soumis à des sanctions de l'UE. En outre, les nouvelles règles visent à renforcer la coopération et la communication entre les autorités compétentes d'un État membre et entre les États membres et les autres institutions, organes, bureaux et agences concernés de l'UE.

60 Directives sur l'application des sanctions financières et les sanctions pécuniaires - GOV.UK 61 Selon les documents judiciaires, BAT Marketing Singapore (BATMS) a plaidé coupable à une information criminelle déposée dans le District de Columbia accusant BAT et BATMS de complot en vue de commettre une fraude bancaire et de complot en vue de violer l'IEEPA. BAT a conclu un accord de poursuite différée lié aux mêmes accusations.

62 Toll a facilité près de 3 000 paiements liés à des expéditions maritimes, aériennes et ferroviaires, en provenance ou à destination de ses unités mondiales, par l'intermédiaire d'institutions financières américaines, au profit de personnes physiques ou morales sanctionnées par les États-Unis ou situées dans des pays sanctionnés par l'ONU ou les États-Unis. Pendant plus de la moitié de la période concernée, la fonction conformité de Toll n'a pas mis en place de politiques et de contrôles proportionnels à la complexité de ses opérations, qui comprenaient près de 600 applications de facturation, de données, de paiement et autres systèmes répartis dans ses différentes unités commerciales. L'action coercitive a révélé qu'après qu'une banque eut soulevé des inquiétudes quant au respect par Toll des sanctions américaines, Toll avait pris des mesures pour atténuer son exposition aux risques en cessant toute activité avec les pays sanctionnés par les États-Unis en juin 2016. Cependant, Toll n'a pas mis en œuvre les politiques et procédures de conformité nécessaires pour empêcher les paiements impliquant des personnes physiques ou morales sanctionnées, ni vérifié si les expéditions impliquaient des personnes situées dans une juridiction sanctionnée par l'ONU ou les États-Unis.

63 Cela exige des pays qu'ils gèlent sans délai les fonds ou autres avoirs de toute personne ou entité désignée par le Conseil de sécurité des Nations Unies ou placée sous son autorité en vertu du Chapitre VII de la Charte des Nations Unies, ou de personnes et entités agissant en leur nom, sur leurs instructions, ou détenues ou contrôlées par elles, et qu'ils veillent à ce qu'aucun fonds ni autre avoir ne soit mis à la disposition, directement ou indirectement, ou au profit de toute personne ou entité désignée par le Conseil de sécurité des Nations Unies ou placée sous son autorité en vertu du Chapitre VII de la Charte des Nations Unies, ou de personnes et entités agissant en leur nom, sur leurs instructions, ou détenues ou contrôlées par elles. À condition que les personnes agissant au nom ou sous le contrôle de personnes et entités désignées, ou détenues ou contrôlées par elles, ne soient pas visées par des régimes de sanctions nationaux ou supranationaux.

Encadré 41. Exemple du Secrétariat du FSRB : GAFILAT organise des exercices de simulation de gel du TFS pour les pays membres

GAFILAT mène des exercices fictifs permettant aux pays membres de tester leurs processus interinstitutionnels de mise en œuvre des TFS conformément aux normes du GAFI. une méthodologie et un manuel développés par GAFILAT, les pays membres répondent à des scénarios destinés à tester les capacités et les mécanismes de contrôle du TFS (y compris ceux en place pour les secteurs public et privé).

Grâce à ces exercices, GAFILAT souhaite fournir aux pays membres un outil pratique pour identifier les faiblesses potentielles et renforcer leurs systèmes de financement du terrorisme. À l'issue de l'exercice, GAFILAT fournit un rapport non public contenant des commentaires et des conseils pour le pays. Depuis 2024, GAFILAT a mené trois exercices simulés impliquant les processus de financement du terrorisme pour trois pays membres. À l'avenir, GAFILAT prévoit d'organiser d'autres exercices simulés, notamment des sessions axées sur les processus de financement du terrorisme pour les autres pays membres.

Source : GAFILAT

133. Dans le contexte des biens à double usage, les autorités de contrôle des exportations sont chargées de réglementer l'exportation de la plupart des articles commerciaux, souvent appelés biens « à double usage », qui sont ceux ayant des applications à la fois commerciales et militaires ou de prolifération.[64] De nombreux pays vont au-delà des exigences du TFS conformément à la résolution 1718 du Conseil de sécurité des Nations Unies et donnent la priorité à la mise en œuvre de réglementations de contrôle des exportations comme outil de gestion des risques plus large contre le PF et l'évasion des sanctions.

Encadré 42. Exemples de juridiction : mécanismes interinstitutions intégrant les réglementations sur le contrôle des exportations

- Inde : Mise en place de multiples mécanismes de coordination opérationnelle et politique sur les PF, notamment le Groupe de travail interministériel (GTI) sur les licences SCOMET (produits chimiques, organismes, matériaux, équipements et technologies spéciaux), qui examine les demandes de licences d'exportation de biens à double usage et les questions connexes. Par ailleurs, le Mécanisme de coordination multi-agences, institué en vertu de la loi indienne sur les armes de destruction massive de 2005, est présidé par la FIU-Inde et comprend la participation des régulateurs, des forces de l'ordre et d'autres organisations compétentes.[65]

64 Des licences d'exportation à double usage sont requises dans certaines situations impliquant la sécurité nationale, la politique étrangère, la pénurie d'approvisionnement, la non-prolifération nucléaire, la technologie des missiles, les armes chimiques et biologiques, la stabilité régionale, la lutte contre la criminalité ou les préoccupations terroristes. Les exigences en matière de licences dépendent des caractéristiques techniques de l'article, de sa destination, de son utilisation finale, de son utilisateur final et de ses autres activités. Même si une licence n'est pas requise, des exigences supplémentaires peuvent être requises avant l'exportation.
Les deux exemples ci-dessous illustrent une attention particulière portée aux réglementations en matière de contrôle des exportations relatives au PF et à l'évasion des sanctions.

65 En vertu des dispositions pertinentes de la loi sur les armes de destruction massive, les différents comités consultatifs indiens sur les armes de destruction massive et leurs Systèmes de livraison, armes nucléaires et articles connexes, armes chimiques et articles connexes, armes biologiques

Singapour : Le Comité interministériel sur le contrôle des exportations (IMC-EC), qui supervise le cadre de contrôle des exportations de Singapour, y compris les questions politiques et opérationnelles liées à la prolifération des armes de destruction massive et des armes de destruction massive. L'IMC-EC est présidé par le ministère des Affaires étrangères et comprend les organismes compétents en matière de politique et d'application de la loi. L'IMC-EC surveille également la mise en œuvre par Singapour des résolutions pertinentes du Conseil de sécurité de l'ONU et coordonne les suivis interinstitutions lorsque Singapour reçoit des informations/renseignements relatifs à la prolifération des armes de destruction massive et des armes de destruction massive.

Sources : Inde et Singapour

134. Comme décrit précédemment dans ce rapport, une compréhension du risque plus large de prolifération des ADM et de son financement sous-jacent pourrait contribuer à la compréhension du risque de violation, de non-application ou de contournement des PF-SFT (c'est-à-dire la définition étroite des risques de PF couverts par les normes du GAFI), et faciliter la mise en œuvre de mesures fondées sur les risques et de PF-SFT. Dans ce contexte, les exemples ci-dessous illustrent un champ d'action plus large de la coordination pour lancer des enquêtes, des poursuites et d'autres mesures complexes en matière de PF et de contournement des sanctions.

Encadré 43. Exemples de juridictions : mécanismes interinstitutions pour faire face aux risques plus larges liés aux PF

- Japon : Dans le cadre du Conseil interministériel pour la politique de LBC, de LFT et de CPF, coprésidé par l'Agence nationale de police et le ministère des Finances, le ministère des Finances et l'Agence des services financiers mènent des « inspections conjointes » où ils mènent conjointement les inspections de change du ministère des Finances et les inspections de LBC de l'Agence des services financiers, dans la perspective de partager les connaissances des agents d'inspection et les informations d'inspection entre les autorités de surveillance respectives et de garantir de manière efficace et efficiente la conformité des institutions financières aux lois et réglementations connexes. En outre, lorsque des navires ou d'autres actifs de la JMSDF (Force maritime d'autodéfense japonaise) détectent des activités suspectées d'être des activités maritimes illicites, y compris des transferts de navire à navire interdits par les résolutions du Conseil de sécurité de l'ONU, le ministère de la Défense fournit les informations aux ministères et agences concernés.
- Malaisie : Il existe deux principaux groupes interinstitutions qui complètent la coopération et la coordination multi-agences du régime CPF de la Malaisie : le Comité d'action commerciale stratégique (STAC), présidé par le Contrôleur du commerce stratégique (STC) au sein du ministère de l'Investissement, du Commerce et de l'Industrie ; et le Comité national de coordination de lutte contre le blanchiment d'argent (NCC), présidé par la Bank Negara Malaysia. Le STAC se concentre principalement sur la mise en œuvre de la loi de 2010 sur le commerce stratégique (STA 2010), qui réglemente les exportations, le transit, le transbordement et le courtage de biens et technologies stratégiques, auxquels participent principalement les organismes chargés de l'application de la loi et les agences techniques liées au blanchiment d'argent.

Les commissions des armes et des articles connexes, ainsi que du contrôle des exportations de biens à double usage, se réunissent régulièrement. Les organisations gouvernementales indiennes concernées y participent afin d'examiner les politiques et les questions connexes relatives aux dispositions pertinentes de la loi sur les armes de destruction massive et d'autres lois gouvernementales indiennes relatives aux armes de destruction massive, à leurs vecteurs et aux biens et technologies à double usage connexes.

Les NCC, qui sont représentés par les ministères et agences compétents en matière de LBC/FT/CPF, formulent, mettent en œuvre et surveillent les stratégies nationales de lutte contre le BC/FT/PF.

- États-Unis : Le service de contrôle des exportations (au sein du Bureau de l'industrie et de la sécurité du ministère du Commerce, BIS) a accès aux données du FinCEN relatives à la loi sur le secret bancaire (BSA), travaille en coopération avec la communauté des exportateurs et mène des enquêtes pour appuyer les sanctions pénales et administratives. Parallèlement, le BIS administre et applique les contrôles à l'exportation des biens à double usage, de certaines munitions et des articles commerciaux par le biais du règlement sur l'administration des exportations (EAR), en vertu de la loi de 2018 sur la réforme du contrôle des exportations (ECRA). Le BIS travaille avec la communauté des exportateurs pour prévenir les violations et mène des enquêtes pour recueillir des preuves à l'appui des sanctions pénales et administratives. Le BIS travaille également en étroite collaboration avec le FinCEN et l'OFAC, ainsi qu'avec les organismes américains chargés de l'application de la loi, pour surveiller les achats illicites par le biais du PF, le contournement des sanctions et le contournement des systèmes de contrôle des exportations.

Sources : Japon, Malaisie et États-Unis

Défis de la coordination interinstitutions

135. Les pays ont signalé divers obstacles à une coordination nationale efficace, mais de nombreuses difficultés étaient liées à un manque général de compréhension et/ou d'adhésion à la gestion des risques de PF, notamment par rapport au blanchiment d'argent et au financement du terrorisme. Les réseaux de PF et de contournement des sanctions étant souvent soutenus par des acteurs étatiques, une communication régulière avec les services de renseignement est nécessaire et l'accès à des informations exploitables est vital pour démasquer les structures d'entreprise sophistiquées et déjouer les plans de contournement des sanctions.

136. Cependant, certains pays ont signalé des obstacles au partage de renseignements, y compris lorsqu'il s'agit de partenaires étrangers qui restreignent l'accès aux informations. Ce défi complique le partage rapide d'informations et la mise en place de mesures immédiates contre les acteurs ou les activités de PF. Dans une juridiction, le manque de compréhension affecte la priorisation de la PF, rendant difficile la mobilisation des autorités compétentes sur le sujet, le partage des informations pertinentes et la réponse rapide aux saisines intergouvernementales.66

137. Certains pays ont signalé un manque de ressources, de connaissances, d'expérience et de technologies pertinentes pour gérer de manière appropriée les risques associés aux stratagèmes de fraude fiscale et d'évasion des sanctions. Bien que de nombreux pays du Réseau mondial du GAFI aient consacré des ressources à la mise à jour de leurs cadres juridiques pour lutter contre la fraude fiscale conformément aux normes du GAFI au cours de la dernière décennie, cela n'a pas conduit à une amélioration notable de la mise en œuvre effective des mesures liées à la fraude fiscale. En avril 2025, alors que plus de la moitié des 194 pays (54 % ; 105 pays) évalués lors du 4e cycle d'évaluation mutuelle étaient conformes (13 % ; 26 pays) ou largement conformes à la R.7 (41 % ; 79 pays), seuls 24 % de ces 105 pays (25 sur 105) ont obtenu des notes très ou substantiellement efficaces au titre de l'IO.11. Au total, 17 % des pays évalués (32 sur 194) ont obtenu des notes très ou substantiellement efficaces sur l'IO.11 (voir figures 1 et 2).

66 Pour ce projet, certains pays ont signalé avoir rencontré des obstacles interinstitutionnels limitant le partage d'informations et d'études de cas pertinentes. Compte tenu de la complexité des systèmes de financement du terrorisme et d'évasion des sanctions, certains pays ont indiqué ne pas être en mesure de déclassifier des renseignements et/ou de partager d'autres informations sensibles avec le reste du réseau mondial du GAFI.

138. Toutefois, dans le contexte de la Recommandation 1, les obligations d'identifier, d'évaluer et de comprendre les risques liés aux PF-TFS mentionnées dans la Recommandation 7 alimentent un effort mondial d'évaluation des risques liés aux PF, ce qui pourrait renforcer l'efficacité dans les années à venir. Plus de la moitié des pays ont déclaré avoir réalisé une évaluation des risques liés aux PF ou un chapitre sur les PF dans leur ENR au cours des cinq dernières années, tandis que près d'un quart des pays procèdent actuellement à leur première évaluation des risques liés aux PF et prévoient de l'achever d'ici fin 2025.

Partage d'informations entre les secteurs public et privé

139. Les partenariats public-privé (PPP) peuvent constituer des plateformes précieuses pour renforcer la collaboration entre les parties prenantes. Ces partenariats visent à permettre aux gouvernements de partager des informations utiles (par exemple, typologies, indicateurs de fraude, bonnes pratiques, défis) avec leurs interlocuteurs du secteur privé. Lorsque le secteur public partage des informations exploitables, le secteur privé est mieux placé pour analyser ses propres dossiers clients et transactions afin d'identifier les activités potentiellement illicites actuelles et passées, y compris les cas de fraude potentielle aux sanctions. Par la suite, ce type d'échange renforce la capacité du secteur public à identifier et atténuer les risques et à émettre des orientations ciblées à l'intention des entités du secteur privé, tout en préservant sa responsabilité de protection de la vie privée des clients.

140. Afin de favoriser le partage d'informations, de nombreux pays ont indiqué avoir élaboré et suivi des indicateurs de risque et des signaux d'alerte concernant les schémas de financement du terrorisme et de contournement des sanctions, en mettant l'accent sur les transactions et les structures commerciales (voir Annexe A : Pertinent pour le financement de la prolifération). En général, les pays partagent la liste des indicateurs de risque avec les secteurs public et privé par le biais d'activités périodiques de sensibilisation. Cependant, près de la moitié des pays n'ont pas indiqué avoir élaboré ou maintenu de tels indicateurs de risque et signaux d'alerte. Cela pourrait indiquer un manque de différenciation entre les indicateurs de risque de financement du terrorisme et d'autres délits financiers, ou un manque de priorité accordée aux cas complexes de financement du terrorisme et de contournement des sanctions dans ces pays. Étant donné que la plupart des pays s'appuient sur les rapports d'alerte et de signalement d'opérations suspectes pour détecter les activités de financement du terrorisme et de contournement des sanctions, il existe un possible déficit d'information entre les secteurs public et privé, ce qui compromet la mise en œuvre efficace des mesures préventives.

Bonnes pratiques pour le secteur public

141. Environ un tiers des pays ont indiqué concentrer leurs efforts sur la sensibilisation du secteur privé par la mise en œuvre de leur cadre juridique relatif aux services financiers transfrontaliers, notamment par la réception de déclarations de soupçon et de déclarations de soupçon et la mise en œuvre immédiate des services financiers transfrontaliers. Cependant, le même nombre de pays ont fait état d'une collaboration plus étroite entre les secteurs public et privé, par le biais de divers PPP dont l'objectif principal n'est généralement pas le financement du terrorisme, bien qu'il existe des groupes de travail ou d'autres mécanismes permettant des discussions sur les questions liées au financement du terrorisme et à l'évasion des sanctions. Certains pays ont également fait état de campagnes de sensibilisation du secteur privé menées par les services de police et de renseignement, outre la participation des ministères des Finances, des CRF et des régulateurs.

Encadré 44. Exemples de juridictions : sensibilisation du secteur public au secteur privé sur le PF et l'évasion des sanctions

- France : Des dispositifs de « sensibilisation » ont été mis en place pour informer et échanger avec le secteur privé, via l'Autorité de contrôle des banques et des assurances (ACBA), rattachée à la Banque centrale, et le Trésor. Outre les institutions financières, les échanges public-privé ciblent principalement les professionnels des secteurs jugés les plus exposés aux risques, notamment les entreprises et professions non financières désignées (EPNFD) et les organisations humanitaires à but non lucratif.

organisations à but non lucratif (OBNL). La CRF organise des réunions ponctuelles spécifiques avec les entités financières françaises (banques et établissements de crédit), dont certaines sont axées sur le financement de la prolifération. Ces entités déclarantes sont les plus importantes pour l'Agence, puisqu'elles représentent 52,6 % des SAR/DOS entrants.
en 2023. Ces réunions ont un double objectif : (i) sensibiliser et (ii) aborder les points sensibles et les problèmes auxquels les banques pourraient être confrontées dans le cadre de la lutte contre le PF. TRACFIN a organisé une série de réunions avec certaines des principales banques françaises afin de mieux comprendre la conformité en matière de PF et d'obtenir un retour d'information sur les défis auxquels elles sont confrontées dans la détection des cas de PF et la mise en œuvre des mécanismes de CPF.

États -Unis : Le BIS du Département du Commerce, qui administre et applique le Règlement administratif sur les exportations (EAR), publie régulièrement des orientations et des avis à l'intention des institutions financières, en coordination avec le FinCEN et d'autres services du gouvernement américain. Ces publications comprennent des signaux d'alerte et des indicateurs de risque pour aider les institutions financières à identifier les transactions potentiellement liées à l'évasion des contrôles à l'exportation américains. Les publications récentes ont porté sur les menaces de financement du terrorisme que représentent l'évasion mondiale des sanctions et des contrôles à l'exportation, les activités de l'Iran liées aux drones et le conflit russo-ukrainien.67,68,69

Sources : France et États-Unis

Défis pour le secteur public

142. Compte tenu de la nature du PF et du contournement des sanctions, ainsi que de l'implication fréquente d'acteurs étatiques et de la collecte de renseignements, ces pratiques impliquent souvent des informations sensibles difficiles à partager publiquement. De nombreux pays ont mis en place des PPP, mais leur objectif principal est généralement d'améliorer l'utilisation efficace des rapports d'activité et des déclarations de soupçon, et il existe peu d'exemples de partenariats spécifiquement axés sur les questions de PF ou de contournement des sanctions. Environ un quart des pays indiquent que la réception de rapports d'activité et de déclarations de soupçon constitue l'étendue de leur action de sensibilisation du secteur privé sur les questions liées au PF et au contournement des sanctions. Cependant, Singapour et le Royaume-Uni ont recours aux PPP pour surmonter certains problèmes de partage d'informations entre les secteurs public et privé, et entre les secteurs privé et privé, concernant le PF et/ou le contournement des sanctions.

Encadré 45. Exemples de juridiction : Surmonter les obstacles au partage d'informations sur le PF et/ou l'évasion des sanctions

Singapour : Le 1er avril 2024, l'Autorité monétaire de Singapour a lancé une plateforme numérique, COSMIC (Collaborative Sharing of Money Laundering/Terrorist Financing Information and Cases), avec six grandes banques commerciales de Singapour. COSMIC permet aux institutions financières de partager en toute sécurité des informations sur les clients présentant plusieurs signaux d'alerte susceptibles de signaler des problèmes de criminalité financière, si les seuils stipulés sont atteints. Cela facilite la détection et la dissuasion des activités criminelles par les institutions financières. COSMIC

Avis conjoint du FinCEN et de la BRI, FIN-2023-NTC2, 6 novembre 2023

68 Microsoft Word - Avis sur l'industrie iranienne des drones - Date limite de publication : 9 juin à 10 h (003)

69 Alerte conjointe FinCEN et Bis pour OCC-OGC-FO

Le COSMIC se concentre actuellement sur trois risques majeurs de criminalité financière dans le secteur bancaire commercial : l'utilisation abusive de personnes morales, l'utilisation abusive du financement du commerce à des fins illicites et le financement de la prolifération. L'objectif du COSMIC est d'aider les institutions financières à identifier les acteurs malveillants et à prendre rapidement des mesures pour perturber les activités et les réseaux illicites, tout en soutenant l'application de la loi et la supervision du système financier.

Royaume - Uni : Le Groupe de travail conjoint de renseignement sur le blanchiment d'argent (JMLIT) est régulièrement utilisé par les services répressifs pour partager des renseignements avec le secteur privé, qui les partage ensuite avec les services répressifs. Cela permet au secteur privé de comprendre les typologies stratégiques et les menaces tactiques. L'Office of Financial Sanctions Implementation (OFSI) a récemment créé une cellule de contournement des sanctions au sein du JMLIT, coprésidée par une institution financière britannique.

Sources : Singapour et Royaume-Uni

Bonnes pratiques pour le secteur privé

143. De nombreuses entités du secteur privé ont indiqué que les PPP sont des outils utiles pour promouvoir le partage d'informations entre les secteurs public et privé et entre les secteurs privé et privé sur les questions d'évasion des sanctions et de PF. Il convient toutefois de noter que le secteur privé a fourni beaucoup plus d'exemples de difficultés que de bonnes pratiques en matière de partage d'informations (voir « Défis pour le secteur privé » ci-dessous). De plus, plusieurs suggestions d'amélioration ont été formulées pour le secteur public.
et développer les initiatives PPP actuelles. Par exemple, les entités du secteur privé ont demandé des processus plus rationalisés pour partager des informations avec les CRF et les forces de l'ordre ; une approche cohérente pour le partage rapide de renseignements du secteur public ; et des cadres juridiques et/ou des orientations plus clairs pour encourager le partage d'informations public-privé dans d'autres domaines.
pays. En outre, certaines entités du secteur privé ont déclaré que l'efficacité du partage d'informations est compromise par un manque de partage intersectoriel. Néanmoins, plusieurs entités du secteur privé estiment que le GAFI pourrait jouer un rôle déterminant dans l'avancement des discussions et l'analyse des risques liés au PF et au contournement des sanctions dans tous les secteurs.

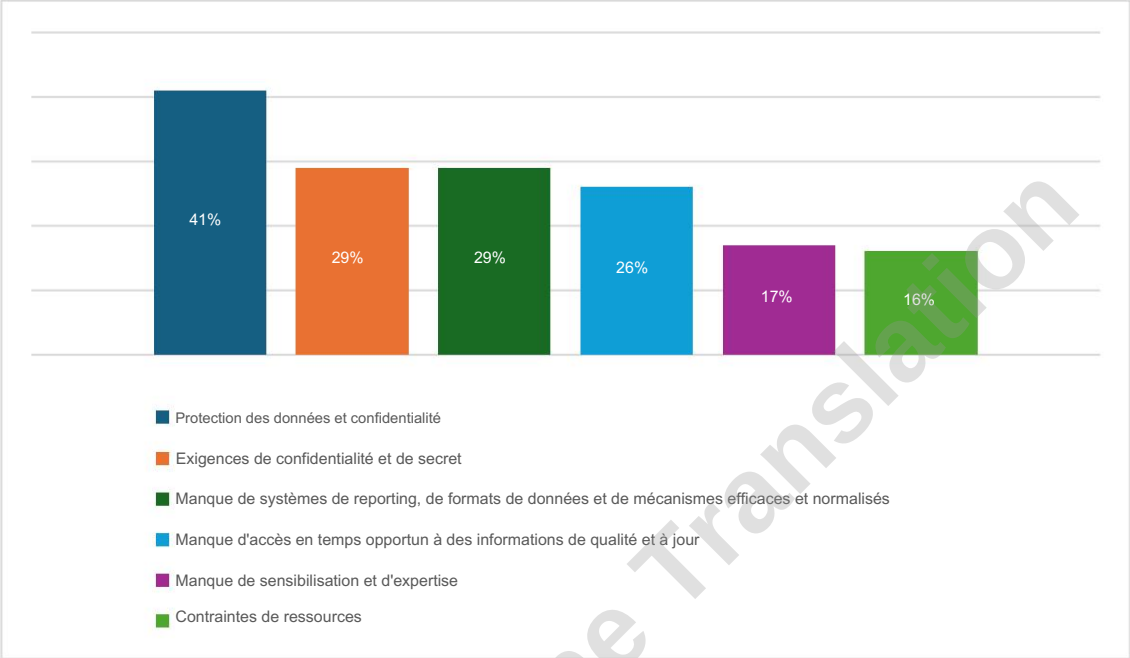
Défis pour le secteur privé

144. Les institutions financières, les EPNFD et les PSAV jouent un rôle important dans la prévention et la lutte contre les stratagèmes complexes de fraude fiscale et de contournement des sanctions. Cependant, les entités du secteur privé ont généralement une compréhension moindre du PF que du BC ou du FT. Par conséquent, la plupart des PPP actuels se concentrent principalement sur la sensibilisation du secteur public au PF et sur la fourniture d'informations sur le dépôt de déclarations de soupçon et de soupçon, ce qui ne permet pas forcément au secteur privé d'apprendre à prendre des mesures concrètes pour identifier et détecter les stratagèmes complexes de fraude fiscale et de contournement des sanctions. Pour détecter et signaler ces stratagèmes complexes, le secteur privé bénéficierait probablement de davantage de conseils sur l'évaluation des activités concernées, telles que le commerce.
transactions et l'échange de grands volumes d'informations entre plusieurs parties.
Les documents pertinents peuvent être stockés sous diverses formes et sur différents supports, ce qui peut rendre difficile le recoupement des données avec les listes de sanctions internationales et nationales.

145. De nombreuses entités du secteur privé ont signalé un certain nombre d'autres pratiques de partage d'informations.
défis, notamment la mise en œuvre inégale des dispositions relatives à la confidentialité des données, d'autres restrictions réglementaires et différences juridictionnelles, des préoccupations en matière de confidentialité et de confiance, des retards dans la diffusion des renseignements, des formats de données incohérents et des contraintes de ressources
(voir figure 4). Le secteur privé a notamment souligné la difficulté de concilier la confidentialité des données et les obligations en matière de mesures préventives. De plus, certaines institutions financières non bancaires

et les DNFBP ont signalé la nécessité d'une orientation sectorielle, puisque la sensibilisation actuelle est davantage axée sur les activités des grandes banques.

Figure 4. Principaux défis en matière de partage d'informations



Coopération internationale

146. Afin de promouvoir une application cohérente des lois et de réduire les possibilités pour les acteurs illicites de cibler les pays ou entités dont les contrôles préventifs sont plus faibles, les secteurs public et privé bénéficient d'une approche harmonisée des cadres juridiques relatifs au financement du terrorisme et au contournement des sanctions. Les normes établies par le GAFI, telles que la mise en œuvre des TFS, et adoptées par les pays, qui peuvent également inclure la criminalisation du financement du terrorisme et le renforcement des contrôles à l'exportation dans certains cas, créent un cadre commun de lutte contre le financement du terrorisme. Par exemple, l'application par les pays de mesures similaires contre l'utilisation abusive des institutions financières réduit le risque de maillons faibles du système financier international. La normalisation des contrôles à l'exportation et la vérification de l'utilisateur final contribuent à empêcher le détournement de technologies sensibles à des fins interdites et à perturber le financement sous-jacent de la prolifération.

147. La coopération internationale est également essentielle pour faire face aux menaces émergentes liées aux nouvelles technologies financières, telles que les actifs virtuels. Dans ce contexte, comme mentionné précédemment, le Groupe de contact du GAFI sur les actifs virtuels a examiné attentivement les défis et les bonnes pratiques pour une mise en œuvre efficace des mesures de LBC/FT/PCF sur les actifs virtuels, en particulier les risques croissants de vol et d'utilisation abusive d'actifs virtuels par la RPDC.

Bonnes pratiques en matière de coopération internationale

148. Certains pays ont indiqué qu'une coopération internationale efficace repose sur l'échange de renseignements entre les gouvernements, les institutions financières et les acteurs du secteur privé. Le partage d'informations sur les transactions suspectes, les entités sanctionnées et les activités à haut risque permet d'identifier et de démanteler les réseaux de financement du terrorisme et les fraudeurs des sanctions. Par exemple, le partage transfrontalier des rapports d'analyse et de signalement (SAR) permet de démasquer des chaînes de transactions complexes liées à la prolifération. Les CRF de la plupart des pays ont déclaré avoir signé des traités et des mémorandums d'accord.

Des protocoles d'accord (MOU) ont été conclus avec d'autres CRF afin de faciliter l'échange de renseignements, notamment ceux relatifs aux activités des PF. Par exemple, le Groupe Egmont de CRF facilite la communication et la collaboration sécurisées entre plus de 160 pays, permettant le partage en temps réel d'informations exploitables.

Encadré 46. Étude de cas : Coopération internationale en matière d'exportation de biens à double usage contrôlés

Le CANAFE a reçu une diffusion spontanée d'une URF détaillant les SAR/DOS
Des informations ont été transmises par des institutions financières de leur juridiction, signalant 90 virements suspects, totalisant environ 2,5 millions de dollars américains. La diffusion spontanée comprenait des virements impliquant des entités soumises au régime de sanctions nationales d'une autre juridiction en raison de l'approvisionnement illicite de biens à double usage pour le secteur de la défense russe. Les rapports d'analyse et de détection des fraudes (SAR) ont identifié plusieurs indicateurs potentiels de blanchiment d'argent et ont identifié plusieurs virements provenant d'entités répertoriées dans la juridiction de la CRF vers des entités au Canada et des entités dans des pays à haut risque d'activités d'approvisionnement illicite.

Le CANAFE a évalué la diffusion spontanée et a produit une déclaration détaillant les activités financières déclarées au CANAFE au moyen de déclarations de soupçons et de déclarations de transactions financières (DOS) et de déclarations de télévirements. La déclaration comprenait des transactions financières entre une entité canadienne et des personnes ou entreprises apparentées ayant déjà fait l'objet d'une enquête en raison de soupçons d'exportation illégale de biens à double usage ou militaires vers des utilisateurs finaux russes. De plus, les DOS et les DOS décrivaient des transactions correspondant à une typologie connue de blanchiment d'argent, notamment des « systèmes de blanchisseries en Russie et en Europe de l'Est », ainsi que des transactions continues avec des entités russes après les sanctions canadiennes.

Les documents de divulgation ont fourni un aperçu d'un réseau présumé d'achats illicites. La déclaration a été envoyée à plusieurs destinataires fédéraux et à d'autres CRF.

Source : Canada

149. La coopération transfrontalière en matière d'application de la loi permet aux pays de s'attaquer à la nature complexe et transnationale du PF et du contournement des sanctions. Les groupes de travail multinationaux renforcent les ressources et l'expertise des autorités gouvernementales pour enquêter sur les réseaux et les démanteler. Par exemple, des opérations coordonnées peuvent permettre de découvrir des sociétés écrans, des intermédiaires et des itinéraires complexes impliquant plusieurs pays, utilisés par des réseaux proliférants pour l'acquisition et le financement de programmes d'armes de destruction massive.

Encadré 47. Étude de cas : La police nationale espagnole coopère avec ses homologues de l'UE pour lutter contre le PF

L'Espagne a récemment été confrontée à plusieurs cas nécessitant une coopération internationale avec d'autres pays de l'UE. Dans chaque cas, des sociétés intermédiaires dissimulaient la destination du matériel. Les entités impliquées étaient des réseaux d'entreprises, certaines possédant des filiales dans différents pays, et leurs dirigeants. Un « facilitateur » ou un intermédiaire intervenait également dans les opérations. Le principal indicateur de risque détecté dans les différents cas était un volume de ventes inhabituel, ainsi que l'origine des transferts et les différents montants détectés après analyse financière.

Dans un cas, la police nationale enquêtait sur le détournement de matériel de défense d'une valeur estimée à 5 millions d'euros vers la Russie, notamment des pièces détachées pour avions militaires, par l'intermédiaire de sociétés écrans et d'intermédiaires. L'enquête a révélé des paiements et un blanchiment de fonds provenant des opérations de vente de ces sociétés écrans. La coopération internationale, dans le cadre des pays de l'UE, a permis d'enquêter sur des expéditions effectuées via des routes et des airs complexes et transitant par différents pays.

Dans une autre affaire, la police nationale enquêtait sur le détournement de substances chimiques d'une valeur de plus de 800 000 euros vers la Russie, une opération interdite par les sanctions de l'Union européenne. Certaines de ces substances étaient des précurseurs d'explosifs et d'armes chimiques. Ces substances chimiques étaient stockées dans une zone franche d'un port espagnol avant d'être exportées. En Espagne, une enquête conjointe a été menée entre la police nationale et les douanes. Le transport s'effectuant par route, une coopération avec les services d'autres pays a été nécessaire pour enquêter sur l'acheminement transfrontalier des substances.

Source : Espagne

Encadré 48. Étude de cas : Les États-Unis et la République de Corée sanctionnent les acteurs qui financent le programme d'armes de destruction massive de la RPDC70

En mars 2024, en coordination avec la République de Corée (ROK), l'OFAC a désigné six individus et deux entités basés en Russie, en Chine et aux Émirats arabes unis, qui génèrent des revenus et facilitent les transactions financières pour la RPDC. Les fonds générés par ces acteurs sont finalement détournés pour soutenir les programmes d'armes de destruction massive de la RPDC, en violation du TFS requis par la résolution 1718 du Conseil de sécurité des Nations unies. La République de Corée a conjointement désigné six de ces mêmes individus et entités pour leur implication dans le financement illicite et la génération de revenus par l'intermédiaire d'informaticiens nord-coréens à l'étranger.

Cette action vise les agents de banques désignées de la RPDC, ainsi que les entreprises qui emploient des informaticiens nord-coréens à l'étranger. Les représentants bancaires, les informaticiens et les entreprises qui les emploient génèrent des revenus et ont accès à des devises étrangères vitales pour le gouvernement de la RPDC. Ces acteurs, opérant principalement via des réseaux situés en Russie et en Chine, orchestrent des stratagèmes, créent des sociétés écrans ou des sociétés-écrans, et

70 Département du Trésor, « Le Trésor sanctionne les acteurs finançant le programme d'armes de destruction massive de la Corée du Nord », (27 mars 2024), Département du Trésor des États-Unis

gérer des comptes bancaires clandestins pour déplacer et dissimuler des fonds illicites, échapper aux sanctions et financer les programmes illégaux d'armes de destruction massive et de missiles balistiques de la RPDC.

Source : États-Unis

150. Certains pays et organisations internationales, comme l'Office des Nations Unies contre la drogue et le crime (ONUDC) et la Banque mondiale, proposent des formations, une assistance technique et des financements pour renforcer les capacités institutionnelles et répressives des pays aux ressources limitées. Ces programmes visent à améliorer les cadres réglementaires, à renforcer les systèmes de surveillance et à sensibiliser les secteurs public et privé aux risques liés au financement de la prolifération. Pour lutter efficacement contre ce phénomène, il est essentiel de fournir une expertise sur la mise en œuvre de contrôles efficaces des exportations et de vérification des utilisateurs finaux, et d'aider les pays à adopter des systèmes de surveillance avancés pour détecter et signaler les activités financières liées à la prolifération.

Encadré 49. Exemple de juridiction : programme européen EU P2P (Partner to Partner)

Le programme P2P (Partner to Partner) de l'UE pour le contrôle des exportations vise à renforcer le contrôle des exportations de biens à double usage et du commerce d'armes dans le monde entier. Géré par la Commission européenne et le Service européen pour l'action extérieure et coordonné par Expertise France, ce programme a pour objectifs de promouvoir et de renforcer la coopération internationale dans le domaine du contrôle des exportations de biens à double usage, de la mise en œuvre du Traité sur le commerce des armes et du contrôle des exportations d'armes, en renforçant les capacités nationales et régionales, en tenant compte de l'équilibre entre les considérations sécuritaires et économiques. Il comprend des activités de sensibilisation aux risques liés au financement de la prolifération et une assistance technique pour la rédaction d'une évaluation nationale des risques liés au financement de la prolifération.

Source : France

Les défis de la coopération internationale

151. Comme indiqué dans d'autres parties du présent rapport, les différences juridictionnelles dans les cadres juridiques et les programmes de sanctions constituent le principal obstacle à une coopération internationale efficace contre les schémas complexes de fraude fiscale et de contournement des sanctions (y compris les différentes approches de la criminalisation de la fraude fiscale, abordées dans les sections « Détection, Enquête et Poursuites »). Les réseaux de fraude fiscale et ceux qui facilitent le contournement des sanctions opèrent au-delà des frontières, exploitant les disparités réglementaires, tirant parti des différents systèmes financiers et du commerce international, constituant une menace pour la sécurité mondiale. Par conséquent, la gestion de ces risques nécessite une coopération internationale solide afin de renforcer la capacité des autorités gouvernementales à prévenir, détecter et perturber les activités illicites. De plus, la coopération entre les pays et les organisations internationales est indispensable, compte tenu du nombre important de pays.

manquent d'infrastructures ou d'expertise pour surveiller et contrer efficacement l'évasion fiscale et les sanctions.

6. Conclusion et domaines prioritaires

152. Alors que de nombreux pays ont réalisé une évaluation des risques liés au PF ces dernières années ou réaliseront la leur d'ici fin 2025, le Réseau mondial du GAFI en est à des stades divers d'identification et d'atténuation des menaces et des vulnérabilités liées aux schémas complexes de PF et de contournement des sanctions. Malheureusement, la lutte conjointe contre et contre le PF et le contournement des sanctions pourrait devenir de plus en plus difficile dans les années à venir. Les acteurs étatiques et non étatiques dotés de ressources suffisantes continueront de rechercher les faiblesses des mesures d'application de la loi, des mesures préventives et des cadres juridiques, et de tirer parti des nouvelles technologies et de l'évolution constante du paysage géopolitique.

153. La meilleure façon de protéger le système financier international contre l'évolution des risques de FP est de renforcer les liens existants et émergents qui constituent les contrôles CPF à travers le monde. Les pays ont réalisé des progrès notables dans la mise à jour de leurs cadres juridiques CPF et la mise en œuvre des FP-TFS au cours de la dernière décennie, mais un bond en avant collectif pourrait être nécessaire dans la mise en œuvre effective des régimes CPF. Dans le contexte des révisions de la Recommandation 1 du GAFI, le Réseau mondial du GAFI dispose déjà d'un plan directeur pour atteindre cet objectif. Comme indiqué dans les Lignes directrices 2021 sur les FP, les pays sont tenus d'identifier, d'évaluer, de comprendre et d'atténuer leurs risques de FP. De plus, les entités du secteur privé sont tenues de mettre en œuvre des processus d'identification, d'évaluation, de suivi, de gestion et d'atténuation des risques de FP, mais elles peuvent le faire dans le cadre de leurs programmes TFS et/ou de conformité existants.[71] [72]
Les pays devraient également déterminer si des efforts supplémentaires peuvent être nécessaires pour faire face aux risques liés aux PF, notamment au moyen d'outils de détection et de signalement, de coordination et de collaboration nationales, d'enquêtes et de poursuites, et de coopération internationale.[73]

154. Cette étude montre que les acteurs du PF et du contournement des sanctions ont fréquemment recours à des intermédiaires pour masquer leurs activités illicites et dissimuler le véritable utilisateur final des biens à double usage et autres articles destinés aux pays proliférants ou sanctionnés. Des stratagèmes sophistiqués sont utilisés pour dissimuler l'identité de ces individus, entreprises et pays.
impliqués dans le contournement des sanctions, ce qui peut compliquer la détection des activités illicites. Afin d'encourager le Réseau mondial du GAFI à œuvrer ensemble pour prévenir et combattre les schémas complexes de fraude fiscale et de contournement des sanctions, plusieurs axes prioritaires doivent être pris en compte.

71 Orientations sur l'évaluation et l'atténuation des risques liés au financement de la prolifération

72 Dans le contexte des risques de FP, les mesures fondées sur les risques mises en œuvre par les institutions financières et les EPNFD visent à renforcer et à compléter la mise en œuvre intégrale des exigences strictes de la Recommandation 7, en détectant et en prévenant la non-application, la violation potentielle ou le contournement des sanctions financières ciblées. Pour déterminer les mesures d'atténuation des risques de FP dans un secteur, les pays devraient prendre en compte les risques de FP associés au secteur concerné. En adoptant des mesures fondées sur les risques, les autorités compétentes, les institutions financières et les EPNFD devraient pouvoir garantir que ces mesures sont proportionnées aux risques.
identifiés, ce qui leur permettrait de prendre des décisions sur la manière d'allouer leurs propres ressources de la manière la plus efficace.

73 Conformément à la Recommandation 2 et à sa Note interprétative, les pays devraient mettre en place un cadre interinstitutions pour atténuer plus efficacement les risques de financement de la prolifération .

Recommandations pour la poursuite des travaux du GAFI sur le CPF

a) Mise à jour périodique sur le PF : Envisager de mettre à jour régulièrement les sections de ce rapport consacrées à la situation actuelle, aux tendances et aux méthodes. Le risque de PF et de contournement des sanctions restera un défi majeur pour le Réseau mondial du GAFI dans un avenir proche. Cependant, les menaces, les vulnérabilités et les typologies qui sous-tendent notre compréhension collective de cette question sont vouées à évoluer et à se remodeler en permanence. Compte tenu de la nature de l'évaluation du risque de PF, il est important que les pays et le secteur privé maintiennent une compréhension du paysage actuel. Sans les rapports d'évaluation des risques de la résolution 1718 du Conseil de sécurité des Nations unies, le GAFI devrait aider les principales parties prenantes à surveiller le paysage des risques.

b) Promouvoir la collaboration entre les secteurs public et privé : Envisager d'utiliser ce rapport et les conclusions de la consultation publique pour structurer la sensibilisation du secteur privé dans le cadre d'un événement du GAFI, puis utiliser leurs commentaires pour élaborer un rapport d'orientation de suivi davantage axé sur les actions pouvant être menées en partenariat avec les institutions financières, les entreprises et professions non financières désignées et les prestataires de services d'investissement VASP afin de renforcer les mesures préventives en matière de CPF. Par exemple, une session ou une série de sessions pertinentes pourraient être organisées pour le Forum consultatif du secteur privé de 2026. Étant donné que le Réseau mondial du GAFI a signalé un recours important aux déclarations d'infraction et aux déclarations de soupçon pour lancer des enquêtes sur les infractions de financement du terrorisme et les sanctions, une sensibilisation et des orientations mieux coordonnées peuvent être utilisées pour renforcer le partage d'informations entre les secteurs public et privé entre les secteurs concernés.

c) Définition des PF ADM : Dans un délai de cinq ans, envisager d'ajouter une définition officielle des PF ADM au Glossaire général du GAFI, en tenant compte des résultats de l'examen horizontal des évaluations des risques de PF du Réseau mondial du GAFI. Comme indiqué dans le présent rapport, les différences juridictionnelles dans l'approche du PF et de l'évasion des sanctions peuvent compromettre ou compliquer la détection, les enquêtes et la coopération internationale sur ce sujet. Une définition unifiée et généralement acceptée atténuerait les frustrations liées à la prévention et à la lutte contre le PF et l'évasion des sanctions.

d) Examen horizontal des ARN des PF : Dans un délai de trois ans, envisager de mener un examen horizontal des évaluations des risques des PF du Réseau mondial du GAFI.

Comme le décrit ce rapport, les pays en sont à des stades différents d'identification, d'évaluation, de compréhension et d'atténuation des risques liés aux FP, et utilisent une série de nouvelles techniques pour y parvenir. De plus, il semble y avoir une compréhension inégale des vulnérabilités liées aux FP et au contournement des sanctions. Compte tenu de l'importance de la tâche qui attend les secteurs public et privé pour mieux comprendre les risques liés aux FP, conformément aux normes du GAFI, une analyse horizontale pourrait contribuer à identifier les bonnes pratiques une fois que le Réseau mondial du GAFI aura eu plus de temps pour évaluer les risques liés aux FP.

Annexe A : Indicateurs de risque

1. Les indicateurs ci-dessous constituent une liste non exhaustive, issue des informations reçues par le GAFI dans le cadre de ce projet. Ils visent à renforcer la capacité des entités des secteurs public et privé à identifier les transactions et/ou activités suspectes liées aux stratagèmes de fraude fiscale et de contournement des sanctions. Bien que plusieurs indicateurs identifiés puissent ne pas sembler avoir de lien direct ou exclusif avec la fraude fiscale ou le contournement des sanctions et puissent être révélateurs d'autres formes d'activités illicites, ils peuvent néanmoins s'avérer pertinents pour identifier les stratagèmes de fraude fiscale et de contournement des sanctions.

Comment utiliser ces indicateurs

2. Un indicateur peut accroître la probabilité d'une activité inhabituelle ou suspecte. L'existence d'un seul indicateur relatif à un client ou à une transaction ne suffit pas à elle seule à justifier une suspicion de fraude fiscale ou de contournement des sanctions, et l'indicateur ne fournit pas nécessairement une indication claire d'une telle activité. Cependant, il peut inciter à une surveillance et un examen plus approfondis, le cas échéant. De même, la présence de plusieurs indicateurs peut également justifier un examen plus approfondi. Le fait qu'un ou plusieurs indicateurs suggèrent une transaction ou une activité suspecte dépend également de l'activité, du produit ou du service proposé par une institution ou un acteur du marché et de la manière dont il interagit avec ses clients.

3. Les indicateurs ci-dessous s'appliquent aux secteurs public et privé. Concernant ce dernier, ils concernent les institutions financières, notamment les banques et les services de transfert de valeurs, les entreprises et professions non financières désignées, les prestataires de services d'actifs virtuels, ainsi que les PME et les grands conglomérats opérant dans le secteur des biens à double usage ou d'autres secteurs concernés. Dans le secteur privé, ces indicateurs sont destinés au personnel chargé de la conformité, du suivi des transactions, de l'analyse des enquêtes, de l'intégration des clients et de la gestion des relations, ainsi que d'autres domaines œuvrant à la prévention du financement du terrorisme, de l'évasion fiscale et des infractions sous-jacentes.

4. Certains indicateurs de risque nécessitent la comparaison croisée de diverses données (par exemple, transactions financières, données douanières) souvent détenues par des sources externes. Du fait de cette dépendance à ces données, le secteur privé peut ne pas observer tous les indicateurs identifiés ci-dessous. Pour certains indicateurs de risque, le secteur privé aura besoin d'informations contextuelles supplémentaires auprès des autorités compétentes, par exemple via des échanges avec les autorités répressives ou les CRF. Lors de l'utilisation de ces indicateurs, les entités du secteur privé doivent également prendre en compte l'ensemble du profil client, y compris les informations obtenues auprès du client lors du processus de due diligence, les modes de financement des transactions, le cas échéant, et d'autres facteurs de risque contextuels pertinents.

5. Le tableau suivant présente les indicateurs de risque regroupés en trois grandes catégories : 1) informations/ comportement des clients ; 2) transactions ; et 3) activités commerciales. Les indicateurs d'information/ comportement des clients peuvent être utilisés pour la conduite des contrôles clients, tandis que les indicateurs de transactions peuvent être utilisés pour le suivi des transactions, y compris les transactions d'exportation. Les activités commerciales peuvent fournir un contexte supplémentaire à prendre en compte dans des processus plus larges de gestion des risques. Bien qu'il existe des chevauchements entre certains indicateurs de risque de chaque catégorie, le Réseau mondial du GAFI a souhaité donner la priorité à la fourniture d'un maximum d'informations afin de soutenir les secteurs public et privé.

1. Informations/comportement du client

1. Utilisation de véhicules d'entreprise (par exemple, des sociétés écrans) pour masquer la propriété, la source des fonds ou les pays/entités impliqués, en particulier les pays sanctionnés.
2. Obscurcir l'utilisateur final grâce à la superposition des transactions, avec des agents d'approvisionnement acheminant les expéditions, les communications et les finances à travers plusieurs couches d'entreprises, de courtiers et d'intermédiaires.
3. Lorsque le client utilise des structures complexes pour dissimuler le lien entre les marchandises importées et exportées, par exemple, il utilise des lettres de crédit à plusieurs niveaux, des sociétés écrans, des intermédiaires et des courtiers.
4. Modifications apportées aux documents commerciaux standards pour masquer le client final.
5. Les informations sur les parties sont similaires à celles des parties répertoriées dans le cadre des sanctions contre les armes de destruction massive ou des contrôles commerciaux (par exemple, noms, adresses ou numéros de téléphone).
6. Les comptes appartiennent à des sociétés aux structures de propriété opaques, des sociétés écrans ou des sociétés d'un jour, ou les transactions sont effectuées par ces sociétés.
7. Le client est impliqué dans la fourniture, la vente ou la livraison de produits à risque restreint ou élevé. biens et/ou technologies.
8. Le client a déjà eu des relations ou entretient des relations avec des personnes ou des entités désormais soumises à des sanctions.
9. Les parties sont physiquement situées dans des pays où le détournement est préoccupant (États qui autorisent la fourniture de biens sensibles à la prolifération, ou leur financement, via leur territoire)
10. Un client ou la contrepartie d'un client effectue des transactions avec des entités et des personnes désignées par le régime national de sanctions, ou des transactions qui contiennent un lien avec des identifiants répertoriés pour les entités et les personnes désignées par le régime national de sanctions, tels que des adresses électroniques, des adresses physiques, des numéros de téléphone, des numéros de passeport ou des adresses de monnaie virtuelle convertible (CVC).
11. Client affilié à des universités et des instituts de recherche gérant des biens à double usage marchandises ou produits soumis au contrôle des exportations.
12. Les transactions impliquent un utilisateur final civil présumé, mais des recherches de base indiquent que l'adresse est une installation militaire ou colocalisée avec des installations militaires dans un pays de préoccupation.
13. Un client acquiert de nouveaux navires sans raison économique ou commerciale apparente.
14. Un modèle d'entreprise est entièrement orienté vers l'exportation et agit comme une entité de passage.
15. L'entreprise opère dans le transport maritime, l'import/export, le textile, l'habillement, la pêche, et/ou l'industrie des produits de la mer.
16. Le client insiste sur la confidentialité des transactions ou montre une préoccupation insuffisante quant à la conformité réglementaire liée aux sanctions et au PF.
17. Les transactions impliquent des entités dont l'enregistrement commercial indique des travaux sur projets « à usage spécial ».
18. Le client demande à emprunter des informations personnelles à ses collègues pour sécuriser contrats.
19. Le client effectue des transactions portant sur des biens qui ne sont pas liés à son activité normale et qui peuvent impliquer des équipements ou des technologies à double usage (par exemple, des réacteurs chimiques, des machines-outils, des composants de systèmes de missiles).

20. Les coordonnées du client, telles que les numéros de téléphone, ne correspondent pas au pays de destination.

21. Un client refuse de fournir des informations aux banques, aux expéditeurs ou à des tiers, y compris des informations sur les utilisateurs finaux, les utilisations finales prévues ou la propriété de l'entreprise.

22. Les entreprises servant de façade à des activités illicites manquent de présence en ligne malgré le traitement de transactions importantes.

23. Usurpation d'adresses électroniques ou Web par des moyens informatiques pour faire croire que des demandes illégitimes proviennent d'entreprises légitimes, souvent en exploitant des relations commerciales connues.

24. L'adresse IP ne correspond pas à l'emplacement indiqué par le client.

25. Une dénomination sociale trop générique, non descriptive ou facilement confondue avec celle d'une autre entité plus connue. De plus, cette dénomination sociale peut être fréquemment mal orthographiée.

2. Transactions

1. Les transactions impliquent des paiements de plus petit volume à partir du même compte bancaire étranger de l'utilisateur final vers plusieurs fournisseurs similaires.
2. Les transactions impliquent un changement de dernière minute dans l'acheminement des paiements qui étaient auparavant programmés à partir d'un pays préoccupant, mais qui sont désormais acheminés via un autre pays ou une autre entreprise.
3. Acheminement d'une transaction interdite via le système financier, obligeant une institution financière à traiter des paiements en violation du régime de sanctions national.
4. Les fonds peuvent circuler de manière cyclique entre les entreprises, l'une cessant le paiement et l'autre initiant le paiement au même bénéficiaire.
5. Un client utilise des services financiers et/ou effectue des transactions qui sont physiquement éloignées du commerce réel de marchandises.
6. Omettre les références aux parties ou aux pays sanctionnés dans les documents relatifs aux transactions financières.
7. Les transactions transitent par des pays ou des centres financiers connus pour leur faible application des sanctions ou pour leur participation à des programmes commerciaux illicites.
8. Utilisation de voies de paiement complexes ou inhabituelles, y compris des chaînes de plusieurs institutions financières, en particulier si elles passent par des pays où les contrôles ou les sanctions en matière de PF sont inadéquats.
9. Transactions qui utilisent des comptes ouverts/lignes de crédit ouvertes pour les paiements en conjonction avec des pays de transbordement connus.
10. Les achats effectués dans le cadre d'une lettre de crédit qui sont consignés à la banque émettrice et non à l'utilisateur final réel.
11. La demande du client d'émettre une lettre de crédit relative à des produits à double usage ou à des produits soumis à un contrôle à l'exportation avant que l'approbation ne soit donnée pour l'ouverture d'un compte.
12. Les montants en circulation des dépôts sur leurs comptes de dépôt ont fortement augmenté, suivis par des retraits d'espèces, ce qui indique la possibilité que de telles transactions soient effectuées.
13. Un client transfère des fonds à l'étranger d'une valeur similaire à celle de dépôts en espèces récents

14. Les clients utilisent des comptes individuels pour le paiement des produits.
15. L'utilisation de nombreux comptes bancaires.
16. Absence de justification claire d'une transaction commerciale ou de raison de payer une somme importante, surtout si elle n'est pas conforme aux activités commerciales normales du client.
17. Le volume et la valeur des marchandises ne correspondent pas au volume des paiements.
18. Le client demande un paiement en actifs virtuels pour échapper aux mesures KYC/AML.
19. Les transferts via des prestataires de services d'actifs virtuels, en particulier s'ils impliquent des pays peu réglementés ou si des échanges décentralisés sont utilisés sans diligence raisonnable appropriée.
20. Utilisation de canaux non officiels ou alternatifs, tels que les systèmes de transfert d'argent (hawala), qui peuvent être utilisés pour contourner les restrictions imposées par les sanctions.
21. Création de nouvelles adresses pour les actifs virtuels afin de créer l'« apparence » de leur non-implication dans les échanges cryptographiques sanctionnés 22.

Transactions liées aux paiements pour des produits de défense ou à double usage provenant d'une société constituée après le 24 février 2022 et basée dans un pays non membre de la Global Export Control Coalition (GECC)

3. Activités commerciales

1. Modification des instructions d'expédition d'un article lorsque l'article arrive dans un centre de fret transitaire, à l'insu de l'exportateur.
2. Modifications de dernière minute des instructions d'expédition qui contredisent l'historique du client ou les pratiques commerciales.
3. Un changement dans les documents d'expédition du destinataire final ou du lieu avant à ou pendant l'expédition.
4. Le client demande une livraison à une adresse non indiquée sur sa pièce d'identité documents.
5. Un produit dont la qualité n'est pas conforme au niveau technologique du le pays de destination est exporté.
6. La ou les transactions impliquent l'expédition de marchandises incompatibles avec les schémas commerciaux géographiques normaux, c'est-à-dire lorsque le pays concerné n'exporte ou n'importe pas normalement ou ne consomme habituellement pas les types de marchandises concernés.
7. Transactions commerciales portant sur des équipements ou des matériaux pouvant être utilisés dans des programmes militaires ou nucléaires (par exemple, alliages à haute résistance, centrifugeuses).
8. Indiquer un transitaire ou un exploitant d'avions charters comme utilisateur final.
9. Les produits sont transportés par des moyens détournés, y compris l'utilisation de un petit navire ou un navire obsolète.
10. Les articles arrivent en petites expéditions fréquentes vers un emplacement central avant d'être combiné.

11. Les transactions impliquent des sociétés de transport de marchandises opérant dans des zones de transbordement à haut risque.
12. Acheminement des achats via des points de transbordement couramment utilisés pour rediriger les articles restreints vers des destinations sous embargo.
13. Transactions associées à des itinéraires d'expédition atypiques pour un produit et destination.
14. Lorsqu'une société de transport de fret/de dédouanement est répertoriée comme la destination finale du produit dans les documents commerciaux.
15. Lorsque le pays de destination/d'expédition des marchandises est différent du pays où les produits sont envoyés/reçus sans aucune raison plausible.
16. Falsification de documents d'expédition, tels que des connaissements et des factures, pour dissimuler les itinéraires de navigation, les ports d'embarquement, les destinataires ou les agents maritimes.
17. Substitution de noms de marchandises soumises à des sanctions ou à des contrôles à l'exportation, ainsi que l'utilisation de faux contrats pour dissimuler l'utilisateur final.
18. Les pièces justificatives, telles qu'une facture commerciale, n'indiquent pas le montant réel utilisateur final.
19. Mauvaise classification des marchandises dans la documentation pour échapper à la détection, par exemple en utilisant des descriptions non sensibles pour des articles restreints.
20. Divergences entre les informations figurant dans les documents commerciaux, de transport et financiers. Par exemple, divergences entre les factures et les informations d'expédition (type de marchandise, poids, valeur, destination).
21. Les exportateurs de la RPDC dissimulent l'origine des marchandises produites en RPDC en apposant des étiquettes indiquant le pays d'origine qui identifient un pays tiers.
22. Les fournisseurs de pays tiers transfèrent des travaux de fabrication ou de sous-traitance vers une usine de la RPDC sans en informer le client ou les autres parties concernées.
23. Les navires marchands battant pavillon de la RPDC ont été physiquement modifiés pour masquer leur identité et se faire passer pour des navires différents.
24. Les produits de luxe sont fréquemment expédiés vers des entrepôts centraux dans des pays tiers. pays.
25. Changements rapides vers de nouveaux acheteurs pour les transactions impliquant un luxe restreint marchandises.
26. L'achat et la livraison de matériaux de construction.
27. Activité financière substantielle sans rapport avec l'objectif commercial déclaré, comme des paiements sans rapport avec les exportations de textiles, de pêche ou de charbon.
28. Les clients qui sont des entreprises de fabrication ou de commerce utilisent des espèces dans les transactions concernant des produits industriels ou d'autres transactions commerciales.
29. Si le prix déclaré de la cargaison est bas par rapport au coût du transport.
30. Le pavillon d'immatriculation d'un navire change fréquemment.

31. Implication des zones franches, qui peuvent être exploitées pour masquer l'origine et le mouvement d'articles sensibles.