LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Justice

# ÉVALUATION VERTICALE DES RISQUES

## FINANCEMENT DU TERRORISME

MAI 2022

Funded by the European Union
NextGenerationEU

# TABLE DES MATIÈRES

**Table des matières** ..... **2**

**1. Introduction** ..... **3**

**2. Champ d'application et méthodologie** ..... **3**

**3. Étapes du financement du terrorisme** ..... **4**

**4. Acteurs terroristes et leurs besoins en matière de financement du terrorisme** ..... **4**

4.1. Acteurs isolés et petites cellules terroristes ..... 4

4.2. Combattants terroristes étrangers (CTE) ..... 5

4.3. Organisations terroristes internationales ..... 6

4.4. Autres acteurs terroristes ..... 6

**5. Évaluation de la menace du financement du terrorisme** ..... **7**

5.1. Contexte ..... 7

5.2. Acteurs isolés, petites cellules et CTE ..... 8

5.3. Organisations internationales et autres acteurs du terrorisme ..... 8

**6. EVALUATION DES SECTEURS VULNERABLES AU FINANCEMENT DU TERRORISME** ..... **11**

6.1. Vulnérabilités sectorielles ..... 11

6.2. Vulnérabilités transversales ..... 12

**7. Analyse des facteurs atténuants** ..... **14**

7.1. Prévention et surveillance ..... 15

7.2. Détection ..... 16

7.3. Poursuite et condamnation ..... 16

7.4. Coopération internationale ..... 17

**8. Risque résiduel** ..... **17**

**Appendix A. Liste des tableaux** ..... **19**

A.1. Liste des tableaux ..... 19

**Appendix B. Acronymes** ..... **20**

B.1. Acronymes ..... 20

**Avertissement :** Veuillez noter que la présente évaluation verticale des risques a été finalisée début février 2022 et a été adoptée par le Comité national de prévention du blanchiment et du financement du terrorisme en mai 2022. Elle ne prend pas en compte l'invasion russe de l'Ukraine et les liens potentiels de FT dans ce contexte.

# 1. INTRODUCTION

Le 15 septembre 2020, le Comité national de prévention du blanchiment et du financement du terrorisme a adopté la première mise à jour de l'évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme (ENR 2020). L'ENR 2020 conclut que les menaces de terrorisme et de financement du terrorisme (FT) sont globalement modérées. Tandis que l'ENR 2020 traite à la fois des risques liés au blanchiment de capitaux (BC) et au FT, la présente évaluation verticale des risques (EVR) se concentre spécifiquement sur le FT afin d'approfondir la compréhension de ces facteurs de risques.

# 2. CHAMP D'APPLICATION ET MÉTHODOLOGIE

Pour réaliser l'évaluation, nous avons suivi l'approche décrite dans la *Terrorist Financing Risk Assessment Guidance* (2019) du Groupe d'action financière (GAFI) pour **évaluer les risques de FT dans les pays dotés de centres financiers et présentant un faible risque domestique de terrorisme**[1]. Ceci renvoie précisément à la situation du Luxembourg.

Tout d'abord, le présent rapport a évalué et classé les différents types d'acteurs terroristes en fonction de leurs besoins financiers variables au cours des différentes étapes du FT (c'est-à-dire la collecte, l'acheminement et l'utilisation des fonds). Plus précisément, alors que les petites cellules, les acteurs isolés et les combattants terroristes étrangers (CTE) ont de faibles besoins financiers, les organisations terroristes internationales se caractérisent par leurs importants besoins financiers.

Ensuite, pour affiner l'analyse, le rapport a étudié les attaques terroristes dans les régions auxquelles le Luxembourg est lié par sa proximité géographique (l'Union européenne (UE) et le Royaume-Uni (RU)) ou par son centre financier (pays tiers).

D'une part, le rapport analyse l'exposition au FT découlant des acteurs isolés et des petites cellules opérant au sein de l'UE et du RU (terroristes liés à l'État islamique d'Irak et au Levant (EIIL) et d'extrême droite). Si certains actes sont liés au terrorisme d'extrême droite, la majorité des attentats ont été perpétrés par des mouvements islamistes et revendiqués notamment par l'EIIL ou par des individus lui ayant prêté serment d'allégeance. A cet égard, les sous-secteurs financiers tels que la banque de détail et le secteur des services de transfert de fonds ou de valeurs (STFV) (qui englobe les établissements de paiement (EP), les établissements de monnaie électronique (EME) et les agents/distributeurs de monnaie électronique agissant pour le compte des EP/EME établis dans d'autres États membres) sont exposés au FT par leurs services spécifiques qui permettent d'acheminer facilement des petites sommes d'argent. D'autre part, le rapport analyse le risque de FT issus des flux de fonds susceptibles d'être acheminés vers ou en provenance d'organisations terroristes internationales étrangères (par exemple l'EIIL) et de transiter par la place financière du Luxembourg.

[1] GAFI, *Terrorist Financing Risk Assessment Guidance*, 2019, paragraphe 39 (lien).

L'analyse est menée en deux étapes. Dans un premier temps, l'évaluation du **risque inhérent** a été réalisée en analysant les menaces de FT[2] ainsi que les sous-secteurs[3] vulnérables au FT. Dans un deuxième temps, les facteurs d'atténuation et leur impact sur la réduction du risque inhérent ont été évalués afin de déterminer le niveau du **risque résiduel**. En outre, le rapport précise le niveau de risque résiduel de chaque étape du FT.

A l'exception de quelques adaptations spécifiques, cette approche est similaire à la méthodologie utilisée dans l'ENR 2020.

En outre, les risques liés aux vulnérabilités transversales sont décrits séparément, sans évaluation du niveau de risque.

# 3. ÉTAPES DU FINANCEMENT DU TERRORISME

Conformément au guide d'évaluation des risques du GAFI, le présent rapport couvre les trois étapes du FT :

1. Des fonds destinés à être utilisés pour soutenir un terroriste ou une organisation terroriste sont **collectés ;**
2. Ces fonds sont ensuite **acheminés** pour financer une activité liée au terrorisme ; et
3. Ces fonds sont **utilisés** pour répondre aux besoins d'un terroriste ou d'une organisation terroriste.

Pour les centres financiers internationaux tels que le Luxembourg, le guide d'évaluation des risques du GAFI indique que « *due to the high volume and cross-border nature of assets managed and transferred, international finance and trade centres may be vulnerable to misuse for the movement or management of funds or assets linked to terrorist activity* ».

# 4. ACTEURS TERRORISTES ET LEURS BESOINS EN MATIERE DE FINANCEMENT DU TERRORISME

Les acteurs du terrorisme diffèrent dans leur organisation, leurs motivations, leurs opérations et leurs activités, et utilisent différents moyens pour collecter, acheminer et utiliser des fonds. Avant d'analyser le niveau de menace du Luxembourg, l'EVR a identifié différents types d'acteurs terroristes ainsi que leurs besoins de financement.

## 4.1. Acteurs isolés et petites cellules terroristes

Bien qu'il n'existe pas de définition unique acceptée d'un acteur terroriste isolé, le présent rapport se base sur une définition pratique établie par le *Royal United Services Institute*, qui se décompose selon les critères suivants :

[2] Selon la définition du GAFI, « *a TF (terrorist financing) threat is a person or group of people with the potential to cause harm by raising, moving, storing or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF (terrorist financing) threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF (terrorist financing) activities, and individuals and populations sympathetic to terrorist organisations* ».

[3] Selon la définition du GAFI, « *the concept of TF (terrorist financing) vulnerability comprises those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type of service that makes them attractive for TF (terrorist financing)* ».

- La violence ou la menace de violence doit être planifiée ou exécutée ;
- L'auteur ou les auteurs doivent agir seuls, à deux ou à trois ;
- L'auteur ou les auteurs doivent agir sans aucun soutien direct dans la planification, la préparation et l'exécution de leur attaque ;
- La décision de l'auteur de passer à l'acte ne doit pas être dirigée par un groupe ou d'autres individus ;
- La motivation ne doit pas être la perspective d'un gain purement personnel et/ou matériel ; et
- La cible de l'attaque doit aller au-delà des victimes qui sont immédiatement touchées par l'attaque.

Le plus souvent, les acteurs isolés et les petites cellules terroristes sont financés par des petites sommes et impliquent des fonds provenant d'activités légitimes, comme par exemple les commerces de détail. Outre les revenus licites issus d'emplois ou d'activités professionnelles, de subventions de l'État et de prestations sociales, les fonds fournis par des personnes partageant la même idéologie peuvent également constituer des sources de revenus pour ces acteurs.

## 4.2. Combattants terroristes étrangers (CTE)

La résolution 2178 du Conseil de sécurité des Nations Unies définit les **CTE** comme « *individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict* »[4]. Les CTE sont l'un des principaux fournisseurs de soutien matériel aux groupes terroristes et représentent donc une menace significative de FT.

En général, les CTE collectent des fonds *via* l'autofinancement ou le financement par les réseaux de recrutement et de facilitation[5]. Pour l'autofinancement, les sources de financement les plus courantes sont les salaires, les prestations sociales, les prêts à la consommation non remboursés, les découverts bancaires et les dons de la famille et des proches. Les réseaux de recrutement et de facilitation ont généralement recours à des recruteurs dédiés qui soutiennent financièrement et matériellement les CTE, notamment en organisant leur transport et en leur achetant des équipements[6].

Les zones de conflit peuvent être atteintes par voie aérienne, maritime ou terrestre via de nombreux itinéraires. Europol considère que la Turquie est une plaque tournante importante pour les CTE en raison de sa proximité géographique avec la frontière syrienne[7] .

Il est difficile de trouver des données actualisées sur le nombre de CTE qui retournent dans leur pays d'origine. D'après un communiqué de presse du Parlement européen de 2017, le Luxembourg figure parmi les Etats membres de l'UE les moins touchés par le phénomène des CTE se rendant dans les zones de conflit (principalement en Syrie et en Irak)[8]. Cependant, il existe quelques cas connus de ressortissants luxembourgeois ayant rejoint l'EIIL ou ses affiliés.

[4] Conseil de sécurité des Nations Unies, *Résolution 2178 (2014)*, 2014, page 2 (lien).
[5] GAFI, *Risques émergents de financement du terrorisme*, 2015 (lien).
[6] GAFI, *Financement de l'organisation terroriste État islamique en Irak et au Levant (EIIL)*, 2015 (lien).
[7] Europol, *European Union Terrorism Situation and Trend Report*, 2021 (lien).
[8] Briefing de presse du Parlement européen : *Combating terrorism*, septembre 2017 (lien).

## 4.3. Organisations terroristes internationales

**Les organisations terroristes internationales** peuvent varier en fonction de leur taille, structure, portée opérationnelle, motivation, recrutement et capacités. Quatre organisations terroristes (notamment : les Talibans, Boko Haram, l'EIIL et Al-Shabaab) ont été responsables de 7 578 décès en 2019, soit environ 55% de tous les décès liés au terrorisme durant cette même année[9]. Comme pour les acteurs isolés, il n'existe pas de profil unique d'organisations terroristes internationales. Cependant, leurs besoins financiers sont généralement très élevés[10]. Elles utilisent les fonds collectés à des fins opérationnelles, de propagande, de recrutement, de formation, de salaire et de rémunération des membres, ainsi que pour des services sociaux (par exemple, santé publique, prestations sociales et éducatives).

De manière générale, les organisations terroristes internationales utilisent diverses méthodes pour collecter des fonds. Elles peuvent le faire par le biais de dons de la part de financeurs privés[11]. Elles peuvent également utiliser les profits issus d'activités criminelles telles que le trafic de stupéfiants, la fraude et la contrebande de marchandises. Comme de nombreuses organisations terroristes internationales occupent de vastes territoires, elles peuvent également collecter des fonds en imposant des taxes et des charges aux entreprises locales, en exploitant des ressources naturelles et en se livrant à d'autres activités criminelles.

## 4.4. Autres acteurs terroristes

Le secrétaire d'État américain définit les **États qui parrainent le terrorisme** comme ceux qui ont « *repeatedly provided support for acts of international terrorism* »[12]. Les **refuges pour les terroristes** sont des zones non gouvernées, sous-gouvernées ou mal gouvernées où les terroristes peuvent « *organise, plan, raise funds, communicate, recruit, train, transit, and operate in relative security because of inadequate governance capacity, political will, or both* »[13]. Ces États et refuges terroristes leur permettent également de collecter ou d'acheminer des fonds. Par exemple, le soutien de l'Iran au Hezbollah a été estimé à 700 millions de dollars par an, ce qui représente la majorité de leur budget annuel[14]. Les États qui parrainent le terrorisme et les refuges pour les terroristes leur permettent également de générer des fonds liés au FT et d'utiliser leurs systèmes financiers pour le transfert de ces fonds. Par exemple, le régime de Assad en Syrie a permis aux banques situées dans les territoires contrôlés par l'EIIL de continuer à fonctionner[15].

**Les « entreprises » terroristes** se trouvent à mi-chemin entre le terrorisme et la criminalité organisée. Bien qu'elles aient une motivation idéologique, leurs opérations financières ressemblent à celles des groupes criminels organisés[16]. Les « entreprises » terroristes ont, par définition, des capacités de financement importantes. Les méthodes que les « entreprises » terroristes peuvent utiliser pour se financer comprennent la fraude, l'enlèvement contre rançon (par exemple, des pirates coopérant avec des groupes djihadistes) et le vol (simple ou qualifié).

---

[9] Institute for Economics and Peace, *Global Terrorism Index*, 2020 (lien).

[10] GAFI, *Emerging terrorist financing risks*, 2015 (lien).

[11] GAFI, *Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL)*, 2015.

[12] Département d'État américain, *State Sponsors of Terrorism*, consulté le 11 mars 2021 (lien), paragraphe 1.

[13] Département d'État américain, *Country Reports on Terrorism*, 2019 (lien), page 204.

[14] Département d'État américain, *Country Reports on Terrorism*, 2019 (lien).

[15] Commission des affaires politiques et de la démocratie, *Financement du groupe terroriste Daesh : leçons apprises*, 2018 (lien).

[16] Royal United Services Institute, *From lone actors to Daesh : rethinking the response to the diverse threats of terrorist financing*, 2018.

# 5. ÉVALUATION DE LA MENACE DU FINANCEMENT DU TERRORISME

## 5.1. Contexte

Afin de déterminer les risques liés au FT, nous avons d'abord analysé la menace terroriste dans l'UE, le RU[17] et dans les pays tiers.

La menace du FT dépend de :

- l'activité terroriste dans une certaine région ; une activité terroriste intense dans une région génère davantage de besoins en matière de FT ; et
- le type de terroristes ou d'organisations terroristes opérant dans cette région ; les acteurs isolés et les petites cellules terroristes nécessitent moins de FT que les organisations terroristes internationales.

Dans cette optique, le rapport a analysé la menace de FT dans certaines régions auxquelles le Luxembourg est lié en raison de sa proximité géographique (l'UE et le RU) ou de son centre financier international (pays tiers).

Le terrorisme est actuellement une menace réelle dans toute l'**Europe.** Les pays proches et voisins du Luxembourg ont été fortement touchés ces dernières années. À l'exception de certains attentats commis par des terroristes d'extrême droite, la majorité des attaques terroristes au cours des cinq dernières années ont été commises par des **petites cellules ou des acteurs isolés liés à l'EIIL**. Même si ces attaques ont été assez nombreuses, leur préparation et leur exécution ont nécessité peu de moyens financiers. D'un point de vue quantitatif, la menace de FT émanant d'acteurs isolés et de petites cellules terroristes dans l'UE est modérée. Cependant les conséquences sont énormes. Afin d'évaluer les vulnérabilités potentielles liées à cette menace spécifique, la présente évaluation des risques a examiné les outils financiers adaptés aux **faibles exigences financières** et leurs prestataires de services.

En outre, les CTE provenant des États membres de l'UE demeurent une source de préoccupation. Si bon nombre des CTE les plus virulents, y compris ceux qui étaient derrière les attentats de Paris de novembre 2015, sont morts à la suite de l'intervention de la coalition anti-EIIL, d'autres ont été emprisonnés lors de la chute des derniers bastions de l'EIIL. Il ne peut être exclu que les survivants et leurs familles cherchent à retourner dans l'UE à la première occasion. Leur rapatriement constitue donc une menace de FT. À cet égard, Europol considère que la Turquie est une plaque tournante importante pour les CTE qui entrent ou sortent de Syrie, étant donné sa proximité géographique avec les zones de conflit et les frontières de l'UE.

Au-delà de l'UE, les régions les plus touchées par les attaques terroristes menées par l'EIIL et ses affiliés sont, selon le *Global Terrorism Index 2020* (GTI 2020)[18], la **région du Moyen-Orient et l'Afrique du Nord** ainsi que **la région subsaharienne**. Malgré le décès du chef de l'EIIL, Abou Bakr al-Baghdadi, en 2019, l'EIIL continue de mener des attaques par le biais de « cellules dormantes » en Irak et en Syrie. À l'échelle mondiale, l'EIIL opère par le biais d'un réseau de groupes affiliés. Le nombre de provinces d'EIIL en dehors de l'Irak et de la Syrie ainsi que le nombre de groupes affiliés qui leur ont prêté serment d'allégeance ou apporté un soutien continue d'augmenter. En 2019, à l'exclusion de l'Irak et de la Syrie, les attaques

[17] Pendant la majeure partie de la période d'observation pertinente pour cette évaluation, le Royaume-Uni était encore un État membre de l'UE.

[18] Institute for Economics and Peace, *Global terrorism index 2020*, (lien).

imputables à l'EIIL ont causé 1 784 morts dans 27 pays. L'influence du groupe a continué à s'étendre en Asie du Sud, ainsi qu'en Afrique subsaharienne par le biais de groupes affiliés à l'EIIL. Tandis que l'EIIL opère dans l'UE principalement par le biais d'acteurs isolés et de petites cellules terroristes, le groupe **opère en tant qu'organisation terroriste** dans les refuges que constituent les vastes régions désertiques du Sahara ou semi-désertiques du Sahel. D'un point de vue quantitatif, leurs besoins en matière de FT sont considérables. Afin d'évaluer les vulnérabilités potentielles liées à cette menace spécifique, la présente évaluation des risques a examiné les outils adaptés à des **besoins financiers très élevés** et leurs prestataires de services.

## 5.2. Acteurs isolés, petites cellules et CTE

Quelle que soit la méthode de collecte de fonds (qu'il s'agisse d'un financement entièrement autonome ou de paiements effectués par des personnes partageant la même idéologie), les acteurs isolés, les petites cellules et les CTE peuvent utiliser des comptes de paiement, des portefeuilles de monnaie électronique, des comptes bancaires ou des actifs virtuels pour acheminer des fonds à des fins de FT ou pour les dépenser en vue de préparer des attaques terroristes.

En ce qui concerne la place financière luxembourgeoise, la principale menace liée aux acteurs isolés et aux petites cellules consiste en l'exploitation et l'utilisation abusive des produits financiers proposés par des entités basées au Luxembourg pour collecter, acheminer et dépenser de petites sommes d'argent à des fins de FT. Il s'agit essentiellement des services financiers de base offerts aux clients locaux et européens par les banques de détail et d'affaires, les EP et les EME.

Bien que les produits financiers de base offerts par les institutions financières luxembourgeoises ne soient pas plus risqués que ceux offerts ailleurs, le Luxembourg est exposé à ce type de risque en raison du nombre important d'entités fournissant ces services. Ceci dit, toutes les institutions financières luxembourgeoises sont entièrement réglementées et supervisées par la Commission de surveillance du secteur financier (CSSF) en matière de lutte contre le BC/FT. La maturité du secteur financier et sa conscience pour la prévention du FT sont significatives. En effet, la Cellule de renseignement financier (CRF), considère que les déclarations d'opérations suspectes (DOS) déposées par les institutions financières luxembourgeoises sont d'une très bonne qualité. Aucun système de paiement alternatif ou non officiel n'a été détecté au Grand-Duché jusqu'à présent.

Pour le Luxembourg, le risque de CTE entrant ou sortant des zones de conflit consiste à retirer de l'argent de comptes luxembourgeois par le biais de distributeurs automatiques de billets (DAB) situés à proximité des zones de conflit en Syrie, en Iran ou en Irak. Cette menace concerne plus particulièrement les régions turques limitrophes de ces pays. L'analyse des retraits aux DAB au cours des deux dernières années dans ces régions montre qu'ils sont plutôt limités (en volume et en valeur). Il est important de noter qu'aucun indice, tel que des TFTR/TFAR[19] liées à ces transactions, ne suggère que ces montants, plutôt faibles, étaient liés au FT ou à des CTE.

## 5.3. Organisations internationales et autres acteurs du terrorisme

Comme mentionné précédemment, les grandes organisations ont non seulement besoin de fonds pour perpétrer des attaques terroristes, mais aussi pour maintenir leur infrastructure, leur propagande et leurs capacités opérationnelles. Elles doivent donc collecter des fonds soit par le biais d'activités criminelles menées par leur organisation (par exemple, trafic en tout genre, extorsion, etc.), soit avec de l'aide des

[19] TFTR est une déclaration d'opérations de financement du terrorisme et TFAR est une déclaration d'activités de financement du terrorisme.

financeurs du terrorisme. La principale menace posée par les organisations terroristes et leurs financeurs consiste en l'utilisation abusive de la place financière luxembourgeoise pour acheminer des fonds plus importants en provenance ou à destination d'organisations terroristes internationales établies dans des régions particulièrement touchées par le terrorisme. Ceci menace les sous-secteurs les plus sophistiqués du secteur financier, principalement la banque privée et le secteur de l'investissement.

L'EVR a estimé que les organisations terroristes opèrent dans des régions caractérisées par une menace terroriste active ou à partir de refuges terroristes. Afin de déterminer l'exposition du Luxembourg et de son centre financier, les étapes suivantes ont été suivies :

1) **Sélection des pays pertinents pour les besoins de cette analyse**. Comme dit précédemment, en ce qui concerne la menace posée par l'EIIL, les pays sélectionnés sont situés à la fois au Moyen-Orient, en Afrique du Nord et dans les régions sub-sahariennes.
2) **Analyse des flux financiers.** Sur les 50 pays sélectionnés, il apparaît que pour la plupart des flux étudiés[20], les trois premiers pays en termes de valeur représentent plus de la moitié des flux analysés.
3) **Analyse des rapports d'évaluation mutuelle** des pays avec lesquelles le Luxembourg entretient des flux financiers importants.
4) **Analyse d'autres variables et flux** (par exemple, la structure démographique du Luxembourg, les importations et exportations, les résidents de ces pays inscrits au registre de commerce et des sociétés ou des bénéficiaires effectifs du Luxembourg, et les organismes à but non lucratif (OBNL) luxembourgeois réalisant des projets de développement et humanitaires dans ces pays).

Les liens avec ces pays sont de deux ordres. Premièrement, d'un point de vue économique, le Luxembourg entretient des relations bilatérales avec certains de ces pays et affiche son attractivité en tant que destination d'affaires. Deuxièmement, en ce qui concerne la coopération au développement et l'aide humanitaire, le Luxembourg a signé des « programmes indicatifs de coopération » avec ses pays partenaires, qui sont des accords-cadres généraux de coopération visant à fournir une aide au développement.

On peut donc conclure que les flux analysés s'inscrivent dans le cadre des relations bilatérales. Le volume et la nature de ces flux n'ont pas révélé de menace concrète pour la place financière du Luxembourg en matière de FT.

[20] Les flux financiers étudiés aux fins du présent rapport sont, entre autres, les dépôts bancaires, les prêts accordés aux résidents des pays sélectionnés, le *correspondent banking*, les investissements dans les banques luxembourgeoises par des résidents de ces pays, les investissements émis par des résidents de ces pays et détenus par des résidents luxembourgeois, les investissements directs étrangers du Luxembourg vers ces pays (et *vice versa*), et les virements électroniques.

# Aperçu n°1

Le tableau ci-dessous fournit un résumé des besoins financiers des différents types d'acteurs du terrorisme et met en évidence, pour chaque type d'acteur, les étapes du FT qui sont susceptibles de se produire au Luxembourg.

**Tableau 1: Résumé des sections précédentes**

| L'activité a lieu terroriste dans... | Type d'acteur du terrorisme | Exigences financières | Étape de FT susceptible de se produire au Luxembourg |
|---|---|---|---|
| **...l'UE et le RU** | Acteurs isolés et petites cellules terroristes | Faibles besoins financiers (<10 000 euros) ; principalement financés par des activités légitimes. | Collecte de fonds (par le biais de revenus légitimes)<br>Acheminement (en abusant des services offerts par la place financière et adaptés à des exigences financières faibles en matière de FT)<br>Utilisation (en exécutant une attaque hypothétique) |
| | CTEs | Faibles besoins financiers (<10 000 euros) ; autofinancement ou *via* des réseaux de recrutement. | |
| **...les pays tiers, en particulier les régions du monde les plus touchées par l'EIIL** | Organisations terroristes internationales et autres acteurs du terrorisme[21] | Besoins financiers élevés | Collecte de fonds (dons de résidents luxembourgeois à des OBNL réalisant des projets de développement et humanitaires à l'étranger)<br>Acheminement (en envoyant des fonds à des organisations terroristes internationales en abusant des services offerts par la place financière et adaptés à des besoins financiers élevés en matière de FT) |
| | « Entreprises » terroristes | | Acheminement (en abusant des services offerts par la place financière et adaptés à des besoins financiers plus élevés en matière de FT) |

[21] Sauf pour les « entreprises » terroristes.

# 6. EVALUATION DES SECTEURS VULNERABLES AU FINANCEMENT DU TERRORISME

## 6.1. Vulnérabilités sectorielles

Les principaux risques en matière de FT pour le Luxembourg émanent de la menace que des acteurs isolés, des petites cellules, des organisations terroristes et leurs financeurs exploitent les vulnérabilités de certains secteurs essentiellement pour acheminer des fonds. L'ENR 2020 contient une étude détaillée des vulnérabilités BC/FT des différents secteurs soumis à la loi du 12 novembre 2004 (Loi LBC/FT de 2004). Les sous-sections suivantes donnent un aperçu détaillé des (sous-)secteurs vulnérables.

Les produits bancaires traditionnels offerts par les **banques de détail et les banques d'affaires** (par exemple, les cartes de débit/crédit, les virements électroniques, les retraits aux guichets automatiques) les rendent vulnérables aux acteurs isolés, aux petites cellules terroristes ou aux CTE qui pourraient en faire un usage abusif pour acheminer des fonds à l'étranger. Il est intéressant de souligner que les activités de banque de détail au Luxembourg se concentrent sur une clientèle locale. Selon une enquête récente menée par la CSSF et l'Association des Banques et Banquiers Luxembourgeois (ABBL) sur l'activité de banque de détail[22,23], la majorité des actifs et passifs sont détenus par des résidents nationaux (88%). Les banques de détail et d'affaires ont déposé le plus grand nombre de DOS : 22 TFAR en 2020 (8 en 2019) et 4 TFTR en 2020 (14 en 2019)[24].

L'exposition **des banques privées** au FT est déterminée par leur taille, leur exposition internationale et la nature de leurs clients (c'est-à-dire la prédominance de comptes potentiellement plus sophistiqués). Le seuil financier requis pour entamer une relation d'affaires et les liens étroits avec les clients (par exemple, les produits sont conçus pour une relation à long terme, le recours à des gestionnaires de clientèle) rendent la banque privée peu attrayante pour les acteurs ayant de faibles besoins financiers. Cependant, des financiers du terrorisme pourraient conclure des contrats de gestion d'actifs ou de patrimoine avec des banques privées luxembourgeoises en vue d'héberger leurs actifs, même si les actifs ou le patrimoine gérés au Luxembourg ne sont pas directement liés au FT.

Comme pour les activités issues de la banque de détail et d'affaires, les produits et services proposés par le secteur des **STFV** permettent un accès facile, rapide et pratique à des transactions transfrontalières. Cela rend le secteur vulnérable aux abus de la part d'acteurs isolés et de petites cellules opérant dans l'UE ainsi que par des CTE. La taille et le volume des transactions des sous-secteurs luxembourgeois des EP et des EME sont importants, alors que seuls quelques agents/distributeurs de monnaie électronique, agissant pour le compte d'EP/EME établis dans d'autres États membres de l'UE, opèrent au Luxembourg[25].

[22] ABBL et CSSF, *Retail banking survey,* 2020 (lien).

[23] Les clients classés comme clients de la banque de détail aux fins de cette étude étaient des particuliers, des professionnels (indépendants, professions libérales, etc.) et des personnes morales (généralement des petites entreprises, etc.), à l'exclusion des entreprises et des clients de la banque privée.

[24] CRF, *Rapport d'activité 2020* (lien).

[25] Alors qu'en 2020, 21 EP/EME traitent 2,5 milliards d'opérations entrantes pour une valeur de 118,1 milliards et 1,5 milliard d'euros d'opérations sortantes pour une valeur de 95 milliards d'euros, le Luxembourg compte 22 agents basés au Luxembourg et 3 distributeurs de monnaie électronique agissant pour le compte d'EP/EME établis dans un autre État membre de l'UE qui traitent 4 millions d'opérations entrantes pour une valeur de 232,7 millions d'euros et 253 932 opérations sortantes pour une valeur de 294 millions d'euros. Ces chiffres importants (en termes de nombre et de volume) s'expliquent par l'importance de la clientèle des EP/EME agréés au Luxembourg.

Comme pour le sous-secteur de la banque privée, l'exposition **du secteur de l'investissement** au FT semble plus importante pour les financeurs du terrorisme en dehors de l'UE que pour les acteurs isolés ou les petites cellules terroristes opérant au sein de l'UE. Cela est particulièrement vrai pour le sous-secteur de la gestion de patrimoine et d'actifs, qui s'adresse généralement à des particuliers fortunés. Néanmoins, il n'y a que peu de preuves que le secteur de l'investissement soit utilisé à des fins de FT, comme le montre le très faible nombre de TFTR/TFAR. Il n'empêche que, comme pour le secteur de la banque privée, la taille du secteur de l'investissement est considérée comme un facteur de vulnérabilité.

Dans les secteurs de la banque privée et de l'investissement, les décisions d'investissement peuvent être prises discrétionnairement. Cela signifie que les décisions d'investissement sont prises par le professionnel et non par le client. Il est donc peu probable que, dans ces secteurs, les fonds soient « acheminés » ou « utilisés » à des fins de FT. Ainsi, il est essentiel de faire la distinction entre les investissements réalisés par un professionnel pour le compte de son client, qui sont en principe indisponibles, et l'utilisation des plus-values qui sont à la disposition du client, sauf si elles sont réinvesties. Les fonds détenus dans le cadre de la banque de détail et d'affaires et par les prestataires STFV ne sont pas soumis à une gestion discrétionnaire, de sorte que les clients peuvent les utiliser pour acheminer des fonds et effectuer diverses transactions.

Globalement, les **OBNL menant des projets de développement et humanitaires à l'étranger** sont exposés à double titre : par les dons qu'ils reçoivent et par la destination de leurs fonds.

- En matière de dons, il arrive que des terroristes ou des organisations terroristes recourent à de faux prétextes pour collecter des fonds. Dans la plupart des cas, les donateurs pensent que l'argent sera utilisé pour financer de véritables activités caritatives. Il arrive aussi qu'ils soient conscients de la véritable destination de leurs fonds et utilisent le prétexte humanitaire pour ne pas éveiller de soupçons. Cette typologie n'a pas encore été identifiée au Luxembourg, mais la vulnérabilité existe ;
- Quant à la destination des fonds, ces derniers peuvent, de manière délibérée ou par inadvertance, être versés par des OBNL actifs dans des projets à l'étranger (avec ou sans statut d'ONGD[26] ) à des terroristes. Ici encore, cette typologie n'a pas encore été identifiée au Luxembourg, mais la vulnérabilité existe.

Bien que ces typologies n'aient pas été détectées au Luxembourg, ce sous-secteur reste très vulnérable compte tenu de la localisation de leurs activités.

## 6.2. Vulnérabilités transversales

Globalement, l'**argent liquide** est le mode de transport le plus fréquemment utilisé à des fins criminelles, y compris pour le FT. Bien que le Luxembourg n'ait pas détecté de groupes terroristes opérant à l'intérieur de son territoire (par exemple, des dons sollicités par des OBNL liées au financement du terrorisme ou par des personnes agissant en leur nom), les risques de FT résultant de l'utilisation d'argent liquide au Luxembourg doivent néanmoins être pris en considération par les entités publiques et privées. Pourtant, il n'existe aucune preuve connue de collecte d'argent liquide à des fins de FT au Luxembourg. Le nombre de déclarations d'argent liquide aux frontières, reçues par l'Administration des Douanes et Accises (ADA), est relativement stable au cours des quatre dernières années. En 2020, la valeur totale représentait 0,02% de la valeur totale de l'argent liquide déclaré aux autorités douanières de l'UE au cours de la même

[26] Les OBNL ayant pour objectif la coopération internationale et le développement (ONGD) sont spécifiquement définies et accréditées par le ministère des Affaires étrangères et européennes (MAEE).

année[27]. Comme mentionné précédemment, la Turquie est considérée comme une plaque tournante importante pour les CTE en raison de sa localisation géographique. L'analyse des retraits aux DAB situés en Turquie liés à des comptes détenus auprès d'institutions financières luxembourgeoises près de la frontière syrienne, iranienne et irakienne montre que ceux-ci étaient plutôt limités. Il est important de noter qu'aucun indice, tel que les TFTR/TFAR liés à ces transactions, ne suggère que ces montants soient liés au FT ou aux CTE.

Les **médias sociaux et les activités de financement participatif (dites *crowdfunding*)** sont vulnérables au FT. Si le marché global du *crowdfunding* au Luxembourg est limité (le volume du marché était estimé entre 1 et 5 millions d'euros en 2015[28] ), une part importante du *crowdfunding* utilise des méthodes de paiement telles que les virements bancaires, les cartes de crédit/débit et les services de paiement par internet[29]. Les banques, les EP et les EME luxembourgeois offrent de tels services à d'autres professionnels à l'étranger. En ce qui concerne les plateformes de *crowdfunding*, le Luxembourg compte une institution offrant des solutions de paiement à ces plateformes. Bien que la part des clients de cette institution impliqués dans le *crowdfunding* soit très limitée, cela pourrait présenter une vulnérabilité potentielle.

Bien que l'évaluation supranationale des risques de 2019 réalisée par la Commission européenne ait reconnu que les risques d'utilisation abusive des **actifs virtuels** pour financer le terrorisme étaient émergents[30], un rapport récent d'Europol indique que le nombre de cas impliquant des actifs virtuels pour le TF reste limité[31]. Au 31 décembre 2021, le Luxembourg compte six prestataires de services d'actifs virtuels (PSAV) enregistrés. Six TFTR/TFAR ont été reportés par des entités liées aux actifs virtuels ou aux PSAV à la CRF en 2020 et 29 en 2021. Rien n'indique que les PSAV luxembourgeois soient exposés de manière significative au FT.

Selon un rapport récent publié par le *Royal United Services Institute*, il apparaît que les nouvelles technologies (par exemple, les médias sociaux, le *crowdfunding*, et les actifs virtuels) n'ont pas joué un rôle prédominant dans le financement de la plupart des attentats terroristes européens (c'est-à-dire ceux menés par des acteurs isolés et des petites cellules). Dans la plupart des cas, les terroristes avaient acheté en espèces ou par d'autres méthodes de paiement bancaire courantes, les instruments pour exécuter les attaques[32]. De manière générale, il a été observé que les groupes terroristes utilisent les actifs virtuels, le *donation-based crowdfunding*, les médias sociaux et les prestataires de services de paiement, en particulier dans les phases de « collecte » et de « d'acheminement »[33]. Toutefois, le rapport indique que les nouvelles technologies se sont ajoutées aux méthodes de financement traditionnelles plutôt que de les remplacer[34].

[27] Commission européenne, *Union douanière - faits et chiffres,* 2020 (lien).

[28] Cambridge Centre for Alternative Finance, *The 2nd European Alternative Finance Industry Report*, 2016.

[29] Groupe Asie/Pacifique sur le blanchiment de capitaux et GAFI du Moyen-Orient et de l'Afrique du Nord, *Social Media and Terrorist Financing*, 2019.

[30] Commission européenne, *Évaluation supranationale des risques,* juillet 2019 (lien).

[31] Europol, *Europol Spotlight : Cryptocurrencies : tracing the evolution of criminal finances,* 2022 (lien)

[32] Royal United Services Institute, *Bit by Bit,* 2022 (lien).

[33] Royal United Services Institute, *Bit by Bit,* 2022 (lien).

[34] Royal United Services Institute, *Bit by Bit,* 2022 (lien).

## Aperçu n°2

Les conclusions tirées dans les sections précédentes sont résumées dans le tableau suivant :

**Tableau 2: Mise en relation des différents acteurs terroristes en fonction de leurs besoins en matière du FT, les étapes du FT qui peuvent potentiellement avoir lieu en Europe (y compris le Luxembourg) et les secteurs vulnérables.**

| | **Activités de FT liées aux CTE, aux acteurs isolés et aux petites cellules terroristes** | **Activités de FT liées aux organisations terroristes internationales et autres acteurs terroristes** |
|---|---|---|
| **Besoins en matière de FT** | Faibles besoins financiers | Importants besoins financiers |
| **Les étapes de FT qui peuvent potentiellement avoir lieu en Europe** | Collecte, acheminement et utilisation[35] | Collecte et acheminement |
| **Secteurs vulnérables au FT** | Banque de détail et d'affaires, STFV | Banque privée, secteur de l'investissement, OBNL réalisant des projets de développement et humanitaires à l'étranger |
| **Vulnérabilités transversales en matière de FT[36]** | Argent liquide, médias sociaux, *crowdfunding,* et actifs virtuels | Médias sociaux, *crowdfunding*, et actifs virtuels |

# 7. ANALYSE DES FACTEURS ATTÉNUANTS

Les risques potentiels moyens ou plus élevés du FT identifiés sont atténués par des contre-mesures, appelées facteurs d'atténuation.

Comme décrit dans l'ENR 2020, l'agencement du cadre de lutte contre le BC/FT repose sur cinq piliers, à savoir : i) la stratégie et coordination nationales, ii) la prévention et la supervision, iii) la détection, iv) les poursuites, les enquêtes et le recouvrement des avoirs, et v) la coopération internationale. Ces piliers reposent sur un cadre juridique exhaustif de lutte contre le BC/FT conforme aux recommandations du GAFI et aux quatrième et cinquième directives anti-blanchiment de l'UE.

[35] Notez que les CTE lèveraient des fonds au Luxembourg et les déplaceraient plutôt à l'étranger avec l'intention de les utiliser dans des pays tiers. Les acteurs isolés et les petites cellules terroristes utilisent généralement les fonds au Luxembourg ou dans l'UE.

[36] Les données disponibles ne permettent pas d'attribuer les vulnérabilités découlant des médias sociaux, du *crowdfunding* et des actifs virtuels à un acteur spécifique. Pour cette raison, et en adoptant une approche conservatrice, ces vulnérabilités transversales sont considérées comme pertinentes pour tous les différents types d'acteurs terroristes étudiés dans le Tableau 2.

## 7.1. Prévention et surveillance

Le Luxembourg est conscient de la nature spécifique des risques de FT décrits ci-dessus. Outre le cadre général de lutte contre le BC/FT, le Grand-Duché a développé des contre-mesures appropriées et spécifiques. Comme expliqué précédemment, le secteur bancaire (et plus précisément la banque de détail, la banque d'affaires et la banque privée), de l'investissement et des STFV, ainsi que les OBNL luxembourgeois menant des projets de développement et humanitaires à l'étranger sont vulnérables au FT. Par conséquent, les facteurs d'atténuation de ces (sous-)secteurs seront analysés dans les paragraphes suivants.

**Les secteurs de la banque, de l'investissement et des STFV** appliquent des mesures d'atténuation similaires. Ils entrent tous dans le champ d'application de la loi LBC/FT de 2004 et de la loi du 19 décembre 2020 relative à la mise en œuvre des mesures restrictives en matière financière (loi de 2020 relative à la mise en œuvre des sanctions). Ils sont donc soumis aux dispositions préventives concernant le BC, le FT et les sanctions financières ciblées. Comme indiqué dans la section concernant les vulnérabilités, ces secteurs sont principalement exposés à travers leurs clients et leurs transactions.

En ce qui concerne les risques liés à la clientèle, le secteur bancaire, de l'investissement et des STFV effectuent leur obligation de vigilance (dite *customer due diligence* ou CDD) avant l'entrée en relation d'affaires et tout au long de celle-ci. Ceci inclut, entre autres, la comparaison automatique de la base de données des clients aux listes de sanctions financières en matière financière.

En ce qui concerne les risques découlant des transactions, ces professionnels ont mis en place des systèmes de surveillance. Plus précisément, les banques, les EP et les EME fournissant des services de commerce électronique ont adopté des systèmes automatisés de suivi des transactions leur permettant de regrouper les transactions, d'identifier les tendances et de partager de manière structurée des rapports de haute qualité (TFTR et TFAR) avec la CRF. Cela permet une coopération plus rapide et plus efficace.

En outre, les prestataires de services de paiement (tels que les professionnels du secteur bancaire et STFV) sont soumis aux obligations du règlement (UE) 2015/847 sur les informations accompagnant les transferts de fonds. Ceci est particulièrement utile pour contrer les risques de FT liés aux acteurs isolés et aux petites cellules terroristes opérant dans l'UE.

Les EP et les EME établis dans un autre Etat membre de l'UE et qui opèrent au Luxembourg par le biais d'**agents/distributeurs de monnaie électronique** doivent nommer un point de contact central au Luxembourg dès qu'ils répondent à des critères spécifiques[37]. Ce point de contact doit assurer une bonne communication et une bonne information conformément aux dispositions prévues aux titres III et IV de la loi de 2009 relative aux services de paiement. Ces points de contact doivent également fournir à la CSSF et aux autorités compétentes de l'Etat membre d'origine des documents et des informations sur demande afin de faciliter la surveillance.

La **CSSF** assure la surveillance de plusieurs types de professionnels en matière de LBC/FT, notamment du secteur bancaire, du secteur de l'investissement et du secteur STFV. Elle effectue des contrôles pour lutter

[37] Conformément aux normes techniques réglementaires conjointes des autorités européennes de surveillance sur les critères permettant de déterminer les circonstances dans lesquelles la désignation d'un point de contact central en vertu de l'article 45 (9) de la directive (UE) 2015/849 est appropriée et les fonctions du point de contact central, les EP et les EME établis dans d'autres États membres, et offrant leurs services par l'intermédiaire d'agents ou de distributeurs de monnaie électronique, désignent un point de contact central entre autres lorsqu'ils opèrent par l'intermédiaire d'au moins 10 agents/distributeurs de monnaie électronique, ou que le volume total des transactions effectuées dépasse 3 millions d'euros, etc.

contre le FT à l'entrée sur le marché et lors de sa surveillance continue. Dans le cadre des contrôles à l'entrée sur le marché, la CSSF effectue des évaluations d'honorabilité et de compétence.

En outre, la CSSF évalue l'activité et le but envisagés lors de l'établissement d'une entité afin de détecter si le professionnel est susceptible d'être abusé à des fins de FT. Par ailleurs, la CSSF a ajouté des contrôles spécifiques pour lutter contre le FT à leur programme de contrôles LBC/FT sur place.

A ce jour, la CSSF n'a détecté aucune violation des sanctions financières ciblées en lien avec le FT, et par conséquent, aucune sanction n'a été imposée. Néanmoins, la CSSF a identifié à plusieurs reprises quelques manquements en matière de surveillance des transactions, de vigilance renforcée et de « *name matching* ». La CSSF sanctionne les manquements qui pourraient être liés au respect des sanctions financières ciblées ou, s'ils sont d'importance mineure, prend des mesures administratives, exigeant une remédiation adéquate par le professionnel.

Bien que les OBNL ne soient pas soumis à la loi LBC/FT de 2004, certains **OBNL luxembourgeois engagés dans des projets de développement et humanitaires à l'étranger** ont mis en place des contrôles spécifiques pour lutter contre le FT. Quelques OBNL ont notamment mis en place des systèmes de vérification de noms tels que *WorldCheck* pour évaluer les niveaux de risque de leurs partenaires et bénéficiaires de fonds. Par ailleurs, les OBNL luxembourgeoises bénéficient des mesures préventives mises en place par leurs prestataires de services. Les systèmes de surveillance des transactions mis en place par les banques lors des virements bancaires n'en est qu'un exemple illustratif.

Enfin, les OBNL luxembourgeoises peuvent demander à obtenir le statut d'organisation non-gouvernementale de développement (ONGD) auprès du ministère des Affaires étrangères et européennes (MAEE) afin de recevoir des subventions pour cofinancer leurs projets à l'étranger. Dans ce cas, le MAEE effectue des contrôles sur les ONGD afin de garantir l'utilisation appropriée des fonds publics. En septembre 2021, le MAEE a publié une mise à jour des conditions générales sur son site internet afin d'y inclure les aspects liés à la lutte contre le FT. En revanche, les OBNL n'ayant pas le statut d'ONGD et qui ne sont pas contrôlés par le MAEE sont exposés à un risque accru de FT.

## 7.2. Détection

La CRF joue un rôle clé dans la **détection** des activités de FT par la réception et l'analyse des DOS et par la dissémination du produit de ses analyses stratégiques et opérationnelles, qui permettent d'identifier les cas de terrorisme et de FT sur base des soupçons rapportés par les déclarants et apportent un soutien aux enquêtes.

Entre 2015 et 2020, la CRF a reçu 1 891 rapports de FT, dont 454 rapports en 2020 et 444 en 2019. Le nombre de rapports FT a augmenté à partir de 2017. L'importante clientèle de certains EP/EME luxembourgeois explique cette envolée. Ces institutions, qui opèrent en ligne, ont de nombreux clients issus de l'UE. Les DOS n'ayant pas de lien direct avec le Luxembourg sont systématiquement partagées avec les cellules de renseignement financier des Etats membres et de pays-tiers concernés.

Le nombre élevé de rapports concernant d'autres pays montre que le secteur privé est conscient des risques liés à la clientèle. La CRF s'efforce d'assurer la meilleure coopération internationale possible avec ses homologues afin de garantir l'efficacité du système.

## 7.3. Poursuite et condamnation

Afin d'empêcher que des crimes liés au terrorisme ne se produisent, toutes les affaires liées font systématiquement l'objet d'une enquête à un stade très précoce.

Comme indiqué précédemment, il n'y a pas de cellules terroristes islamiques qui opèrent au Luxembourg et seuls quelques CTE ont quitté le pays pour rejoindre l'EIIL en Syrie. Bien que surveillés de près, aucun d'entre eux n'est encore revenu. En 2021, les premières poursuites et condamnations ont eu lieu au Luxembourg pour des actes liés au terrorisme islamique. Le faible taux de poursuites et de condamnations démontre le succès de la stratégie luxembourgeoise d'enquête précoce.

## 7.4. Coopération internationale

Compte tenu de l'économie ouverte et de la place financière du Luxembourg, les autorités nationales assurent une **coopération internationale** diligente dans le domaine du FT. Cela inclut la coopération de la CRF avec ses homologues étrangers, la coopération policière par le biais d'Europol et d'Interpol, la coopération des autorités judiciaires par le biais de demandes d'entraide judiciaire et la coopération des superviseurs avec leurs homologues internationaux.

# 8. RISQUE RÉSIDUEL

En tenant compte des vulnérabilités sectorielles et des facteurs d'atténuation en place, le tableau ci-dessus résume le risque résiduel des différents (sous-)secteurs évalués dans l'EVR de FT.

**Tableau 3: Résumé des facteurs d'atténuation des secteurs et sous-secteurs et évaluation du risque résiduel**

| Secteur | Sous-secteur | Risque FT inhérent | | Risque FT résiduel |
|---|---|---|---|---|
| **Banques** | Banque privée | **Modéré** | | **Faible** |
| | Banque de détail et d'affaires | **Elevé** | | **Modéré** |
| **Secteur de l'investissement** | Gérants de fortune | **Modéré** | | **Faible** |
| | Placement collectifs | | | |
| **Services de transfert de fonds ou de valeur (STFV)** | Etablissement de paiement | **Elevé** | *Impact des facteurs d'atténuation* | **Modéré** |
| | Etablissement de monnaie électronique | | | |
| | Agents et distributeurs de monnaie électronique agissant pour le compte de EP/EME établis dans d'autres États membres européens | | | |
| **Organismes à but non lucratif réalisant des projets de développement et humanitaires à l'étranger** | OBNL (Associations sans but lucratif et fondations) réalisant des projets de développement et humanitaires à l'étranger | **Elevé** | | **Elevé** |

Pour conclure, les sections suivantes détaillent le risque TF résiduel au Luxembourg aux trois étapes FT : la collecte, l'acheminement et l'utilisation des fonds.

**Tableau 4 : Conclusion**

| | Collecte | Acheminement | Utilisation |
|---|---|---|---|
| **Banque de détail et d'affaires** | Les petites cellules, les acteurs isolés et les CTE peuvent collecter des fonds d'origine légitime tels que des salaires, des prestations sociales, des prêts non remboursés ou des découverts. | Les services financiers de base (par exemple, les virements électroniques et les retraits aux guichets automatiques) peuvent être abusés pour transférer des fonds destinés au terrorisme vers des petites cellules, des acteurs isolés et des CTE. | Les petites cellules, les acteurs isolés et les CTE peuvent utiliser des fonds pour commettre des actes terroristes. |
| **Banque privée**<br>**Secteur de l'investissement** | Pertinence pour les financeurs du terrorisme en dehors de l'UE | La gestion d'actifs discrétionnaire ne convient pas pour transférer des fonds à des fins de FT. Les fonds gérés par le gestionnaire d'actifs dans le cadre d'un contrat discrétionnaire sont inaccessibles au client.<br>Les revenus générés qui ne font plus l'objet d'une gestion discrétionnaire peuvent être transférés à des terroristes ou à des organisations terroristes. | Non applicable tant que les fonds sont sous gestion discrétionnaire.<br>Cela n'empêche pas le secteur de l'investissement d'exercer le devoir de vigilance (renforcée) sur les projets d'investissement dans les régions touchées par le terrorisme et sur les entreprises opérant dans ces régions. |
| **STFV** | Les petites cellules, les acteurs isolés et les CTE peuvent abuser des fournisseurs STFV pour collecter des fonds à des fins de FT (y compris les paiements liés aux services de *crowdfunding*). | Les STFV peuvent être abusés pour transférer des fonds destinés au FT vers des petites cellules, des acteurs isolés et des CTE. | Les petites cellules, les acteurs isolés et les CTE peuvent utiliser des fonds pour commettre des actes terroristes. |
| **OBNL réalisant des projets de développement et humanitaires à l'étranger** | Les OBNL peuvent collecter des fonds (de manière délibérée ou par inadvertance) à des fins de FT. | Certains pays à haut risque n'ont qu'un accès limité aux systèmes de correspondants bancaires internationaux et certains OBNL menant des projets de développement et humanitaires à l'étranger peuvent être tentés d'utiliser des canaux informels ou non réglementés (par exemple, Hawala ou autres prestataires de services) pour transférer des fonds vers ces pays.<br>Aucune preuve de l'existence de Hawala ou d'autres prestataires de services opérant au Luxembourg. | Non applicable, sauf pour les OBNL qui collectent, de manière intentionnelle, des fonds à des fins de FT. |

# APPENDIX A. LISTE DES TABLEAUX

## A.1. Liste des tableaux

Tableau 1: Résumé des sections précédentes ..... 10
Tableau 2: Mise en relation des différents acteurs terroristes en fonction de leurs besoins en matière du FT, les étapes du FT qui peuvent potentiellement avoir lieu en Europe (y compris le Luxembourg) et les secteurs vulnérables. ..... 14
Tableau 3: Résumé des facteurs d'atténuation des secteurs et sous-secteurs et évaluation du risque résiduel ..... 17
Tableau 4 : Conclusion ..... 18

# APPENDIX B. ACRONYMES

## B.1. Acronymes

| **Acronyme** | **Définition** |
|---|---|
| ABBL | L'Association des Banques et Banquiers, Luxembourg |
| ADA | Administration des Douanes et Accises |
| BC | Blanchiment de capitaux |
| CRF | Cellule de Renseignement Financier |
| CSSF | Commission de Surveillance du Secteur Financier |
| CTE | Combattant terroriste étranger |
| DAB | Distributeurs automatiques de billets |
| DOS | Déclaration d'opération suspecte |
| EMI | Etablissement de monnaie électronique |
| ENR | Evaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme |
| EIIL | Etat islamique d'Irak et au Levant |
| EP | Établissement de paiement |
| EVR | Évaluation verticale des risques |
| FT | Financement du terrorisme |
| GAFI | Groupe d'action financière |
| GTI 2020 | *Global Terrorism Index* 2020 |
| ISIL | État islamique d'Irak et au Levant |
| LBC/FT | Lutte contre le blanchiment de capitaux et le financement du terrorisme |
| MAEE | Ministère des Affaires étrangères et européennes |
| OBNL | Organisme à but non lucratif |
| ONGD | Organisation non gouvernementale pour le développement |
| PSAV | Prestataires des services d'actifs virtuels |
| RU | Royaume-Uni |
| STFV | Services de transfert ou de valeur monétaire |
| TFAR | Déclaration d'activités de financement du terrorisme |
| TFTR | Déclaration d'opérations de financement du terrorisme |
| UE | Union européenne |