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

TERRORIST FINANCING

VERTICAL RISK ASSESSMENT

MAY 2022

Funded by the European Union
NextGenerationEU

TABLE OF CONTENTS

Table of Contents **2**

1. Introduction **3**

2. Scope and methodology **3**

3. Terrorist financing stages **4**

4. Terrorism actors and their terrorist financing needs **4**

4.1. Lone actors and small terrorist cells 4

4.2. Foreign terrorist fighters 5

4.3. International terrorist organisations 6

4.4. Other terrorist actors 6

5. Assessing the terrorist financing threat **7**

5.1. Context 7

5.2. Lone actors, small cells and foreign terrorist fighters 8

5.3. International organisations and other terrorist actors 8

6. Assessing terrorist financing vulnerable sectors **11**

6.1. Sectoral vulnerabilities 11

6.2. Cross-sectoral vulnerabilities 12

7. Mitigating factor analysis **14**

7.1. Prevention and supervision 15

7.2. Detection 16

7.3. Prosecution and conviction 16

7.4. International cooperation 17

8. Residual risk **17**

Appendix A. List of tables **19**

A.1. List of tables 19

Appendix B. Accronyms **20**

B.1. List of acronyms 20

Disclaimer: Please note that this vertical risk assessment was finalised at the beginning of February 2022 and was adopted by the Committee on the Prevention of Money Laundering and Terrorist Financing (the Prevention Committee) in May 2022. It does, therefore, not refer to the Russian invasion in Ukraine and potential TF in that context.

1. INTRODUCTION

On 15 September 2020, the Prevention Committee adopted the first update of the national risk assessment of money laundering and terrorist financing (2020 NRA). The 2020 NRA concludes that the threats of terrorism and terrorist financing (TF) are moderate overall. While the 2020 NRA covers both money laundering (ML) and TF, this vertical risk assessment (VRA) solely focuses on TF in order to deepen the understanding of its drivers.

2. SCOPE AND METHODOLOGY

To conduct the assessment, we followed the approach outlined in the Financial Action Task Force (FATF) TF Risk Assessment Guidance (2019) for **assessing TF risks in jurisdictions with financial centres and low domestic terrorism risk**, which is suitable for Luxembourg's particular situation[1].

Firstly, this report assessed the different kinds of terrorist actors and categorized them according to their varying financial needs throughout the different stages of TF (i.e., raising, moving and using). More precisely, whereas small cells, lone actors and foreign terrorist fighters (FTFs) have low financial needs, international terrorist organisations are characterised by their important financial requirements.

Secondly, in order to streamline the analysis, the report analysed the terrorist attacks in certain regions to which Luxembourg is connected through its geographical proximity (the European Union (EU) and the United Kingdom (UK)) or its financial centre (third countries).

On the one hand, the report analyses the TF exposure arising from lone actors and small cells operating within the EU and the UK (Islamic State of Iraq and the Levant (ISIL)-related and extreme right-wing terrorists). While certain acts were related to extreme right-wing terrorism, the majority of the attacks were carried out by the Islamist movement and claimed in particular by ISIL or by individuals who pledged allegiance to it. This TF exposure typically materialises by much smaller movements of funds channelled through specific services of the financial sub-sectors, such as retail banking and the money value or transfer services (MVTS) sector (which encompasses for Luxembourg payment institutions (PI), e-money institutions (EMI) and agents/e-money distributors of PIs/EMIs established in other Member States). On the other hand, the report analyses the TF risk arising from large flows of funds that may be channelled to or from foreign international terrorist organisations (e.g. ISIL) and transit through Luxembourg's financial centre.

[1] FATF, *Terrorist Financing Risk Assessment Guidance*, 2019, paragraph 39 (link).

The analysis is conducted in two steps. As a first step, the **inherent risk** assessment was performed by analysing TF threats[2] in Luxembourg, and sub-sectors' vulnerabilities[3] to TF abuse. As a second step, mitigating factors and their impact on inherent risk reduction were assessed, resulting in a **residual risk**. Furthermore, the report concluded on the residual risk level of each stage of TF.

This approach is similar to the methodology used in the 2020 NRA, with specific adjustments.

In addition, the risks of cross-sector vulnerabilities are described separately, without a rating assessment

3. TERRORIST FINANCING STAGES

In line with the FATF TF Risk Assessment Guidance, this report covers all three stages of TF:

1. Funds intended to be used to support a terrorist or a terrorist organisation are **raised;**
2. Those funds are then **moved** to finance a terrorism-related activity; and
3. Ultimately, those funds are **used** to meet the needs of a terrorist or terrorist organisation.

For international financial centres such as Luxembourg, the FATF TF Risk Assessment Guidance states that "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. TERRORISM ACTORS AND THEIR TERRORIST FINANCING NEEDS

Terrorism actors differ in their organisation, motivations, operations and activities, and use different means to raise, move and use funds. Before analysing the TF threat level in Luxembourg, this risk assessment identified the following main types of terrorism actors, as well as their financing requirements:

4.1. Lone actors and small terrorist cells

While there is no single accepted definition of **lone-actor terrorism**, this report refers to a working definition established by the Royal United Services Institute that has been broken down into the following inclusion criteria:

- Violence, or the threat of violence, must be planned or carried out;
- The perpetrator(s) must be an individual, dyad or triad;
- The perpetrator(s) must act without any direct support in the planning, preparation and execution of the attack;
- The perpetrator's decision to act must not be directed by any group or other individuals;

[2] As per the FATF definition, "a TF 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 threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations."

[3] As per the FATF definition, "the concept of TF 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."

- The motivation cannot be purely personal-material gain; and
- The target of the attack extends beyond those victims who are immediately impacted by the attack.

Lone actors and small terrorist cells are mostly funded through small amounts and involve funds usually sourced from legitimate activities, such as retail businesses, amongst others. In addition to licit employment incomes, state subsidies and social benefits, funds provided from like-minded individuals within the community, can also be sources of income for these actors.

4.2. Foreign terrorist fighters

The United Nations Security Council resolution 2178 defines **foreign terrorist fighters (FTFs)** as "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] FTFs are one of the primary providers of material support to terrorist groups and thus pose a significant TF threat.

Globally, the two most common methods for FTFs to raise funds are self-funding and funding by recruitment and facilitation networks[5]. For self-funding, the most common funding sources include salaries, social benefits, non-paid-off consumer loans, overdraft from bank accounts and donations from family and friends. Recruitment and facilitation networks will typically have specific recruiters that support FTFs financially and materially, including arranging transportation and purchasing supplies[6].

Travel routes to reach conflict zones areas are either by air, sea or land and involve multiple connections. Europol considers Turkey to be a major transit hub for FTFs given its geographical proximity to the Syrian border[7].

It is difficult to find updated data on the number of FTFs returning to their home country. According to a 2017 press briefing of the European Parliament, Luxembourg is one of the countries in the EU least affected by FTFs travelling to conflict zones (mostly Syria and Iraq)[8]. However, there are a few known cases of Luxembourg nationals having joined the ISIL or its affiliates.

[4] United Nations Security Council, *Resolution 2178 (2014)*, 2014, page 2 (link).
[5] FATF, *Emerging terrorist financing risks*, 2015 (link).
[6] FATF, *Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL)*, 2015 (link).
[7] Europol, *European Union Terrorism Situation and Trend Report*, 2021 (link).
[8] European Parliament press briefing: Combating terrorism, September 2017 (link).

4.3. International terrorist organisations

International terrorist organisations can differ in size, structure, operational reach, motivation, recruitment and capabilities. Four terrorist organisations, the Taliban, Boko Haram, ISIL and Al-Shabaab, together were responsible for 7 578 deaths in 2019, or approximately 55% of all terrorism-related deaths that year[9]. Similar to lone actors, there is no one single profile for international terrorist organisations. However, the financial requirements to maintain them are typically very high[10]. They use raised funds usually for operations, propaganda, recruitment, training, salaries and member compensation, and social services (e.g. health, social and educational provision).

Globally, international terrorist organisations use a variety of methods to raise funds. They may raise funds through private donations, and wealthy private donors may form an important source of income[11]. They may also use proceeds of criminal activity, such as drug trafficking, fraud and smuggling of goods. As many international terrorist organisations occupy vast territories, they may raise funds through imposing taxes and fees on local businesses, exploiting natural resources and other criminal activities.

4.4. Other terrorist actors

The US Secretary of State defines **State sponsors of terrorism** as those that have "repeatedly provided support for acts of international terrorism"[12]. **Terrorist safe havens** include ungoverned, under-governed or ill-governed physical areas where terrorists can "organise, plan, raise funds, communicate, recruit, train, transit, and operate in relative security because of inadequate governance capacity, political will, or both" [13]. State sponsors of terrorism and terrorist safe havens can enable terrorists to raise or move funds. For example, Iran's support to Hezbollah has been estimated to reach up to $700 million per year, accounting for the majority of Hezbollah's annual budget[14]. State sponsors of terrorism and terrorist safe havens can also promote illicit activities that generate funds for terrorists or allow their financial systems to be misused for moving funds. For example, the Assad regime in Syria allowed banks in territories controlled by ISIL to continue operating[15].

"Corporate" terrorist groups sit in an area between that of terrorism and organised crime. While they have a professed ideological motivation, their financial operations resemble those of organised criminal groups[16]. "Corporate" terrorist groups, by definition, have advanced and significant financing capabilities. Methods that "corporate" terrorist groups might use for financing include fraud, kidnapping for ransom (e.g. pirates cooperating with jihadist groups), robbery and theft.

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

[10] FATF, *Emerging terrorist financing risks*, 2015 (link).

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

[12] US State Department, *State Sponsors of Terrorism*, retrieved 11 March 2021 (link), paragraph 1.

[13] US State Department, *Country Reports on Terrorism*, 2019 (link), page 204.

[14] US State Department, *Country Reports on Terrorism*, 2019 (link).

[15] Committee on Political Affairs and Democracy, *Funding of the terrorist group Daesh: lessons learned*, 2018 (link).

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

5. ASSESSING THE TERRORIST FINANCING THREAT

5.1. Context

In order to determine TF-related risks, the terrorist threat in the EU (including UK)[17] and in third countries was analysed first.

The TF threat depends on:

- the terrorist activity in a certain region; intense terrorist activity in one region creates need for more TF; and
- the type of terrorists or terrorist organisations operating in that region; lone actors and small terrorist cells need less TF than international terrorist organisations.

Having this in mind, the report analysed the TF threat in certain regions to which Luxembourg is connected through its geographical proximity (the EU and the UK) or its international financial centre (third countries).

Terrorism is currently a real threat across **Europe.** Countries near or neighbouring Luxembourg have been significantly impacted in recent years. With the exception of certain attacks committed by extreme right-wing terrorists, a large proportion of terrorist attacks carried out during the last five years were perpetrated by **small cells or lone actors related to ISIL**. Even though these attacks were quite numerous, their preparation and execution required few financial means. From a quantitative point of view, the TF threat emanating from lone actors and small terrorist cells within the EU is moderate. However, its consequences are tremendous. In order to assess potential vulnerabilities related to that specific threat, this risk assessment looked into instruments fit for **small financial requirements** and their service providers.

Moreover, FTFs from EU Member States continue to be a source of concern. While many of the most aggressive FTFs, including those behind the perpetrators of the Paris attacks of November 2015, have died as a result of raids by the anti-ISIL coalition forces, others were taken prisoner when the last strongholds of ISIL fell. It cannot be excluded that survivors and their families will seek to return to the EU at the earliest opportunity and therefore there is a related TF threat in relation to their repatriation. In this regard, Europol considers Turkey to be a major transit hub for FTFs entering or leaving Syria given its close geographical proximity to conflict zones and the EU borders.

Looking beyond the EU, those regions most impacted by terrorism attacks conducted by ISIL and its affiliates according to the Global Terrorism index 2020 (GTI 2020)[18] are the **Middle East region and Northern Africa and Sub Saharan region**. Despite the death of the ISIL leader Abu Bakr al-Baghdadi in 2019, ISIL continues to conduct attacks through "sleeper cells" in Iraq and Syria and globally through a network of affiliated groups. The number of ISIL provinces outside of Iraq and Syria continues to rise, as does the number of affiliate groups that have pledged allegiance or support to the core group. In 2019, ISIL-related attacks occurred in 27 countries, excluding Iraq and Syria, resulting in 1 784 fatalities. The group's influence has continued to push into South Asia, as well as sub-Saharan Africa via ISIL-affiliated groups. Thus, while ISIL operates in the EU mainly through lone actors and small terrorist cells, it **operates as a terrorist organisation** in the safe havens provided by the vast deserted regions of the Sahara or the

[17] For most of the observation period relevant for this assessment UK was still an EU Member State.

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

semi-deserted regions of the Sahel. From a quantitative point of view, the TF needs for ISIL and its affiliates in these regions are very high. In order to assess potential vulnerabilities related to that specific threat, this risk assessment looked into instruments fit for **very high financial requirements** and their service providers.

5.2. Lone actors, small cells and foreign terrorist fighters

Regardless of the method of fundraising (whether entirely self-funded or through payments from like-minded individuals), lone actors, small cells and FTFs may use payment accounts, e-money wallets, bank accounts or virtual assets to channel funds for TF purposes or to spend them in preparation for terrorist attacks.

With regard to Luxembourg's financial centre, the main threat in relation to individual terrorists and small cells consists of the exploitation and misuse of financial products offered by Luxembourg-based entities to collect, transfer and spend small amounts of money for TF purposes. This essentially concerns basic financial services offered to local and EU customers by retail and business banking, PIs and EMIs.

Although basic financial products offered by Luxembourg financial institutions are not riskier than those offered elsewhere, Luxembourg is exposed to this type of risk due to the number of entities providing such services. This being said, all Luxembourg financial institutions are fully regulated and supervised for anti-money laundering and countering terrorist financing (AML/CFT) purposes by the Financial Supervisory Authority, the *Commission de Surveillance du Secteur Financier* (CSSF). The maturity and awareness for preventing TF of the financial sector is significant. Indeed, the Luxembourg Financial Intelligence Unit, the *Cellule de Renseignement Financier* (CRF), considers the quality of the suspicious transaction reports (STRs) filed by Luxembourg financial institutions as high. No alternative or unofficial payment system has been detected in Luxembourg so far.

For Luxembourg, the TF risk posed by FTFs entering or leaving conflict zones consists of the withdrawal of cash from Luxembourg accounts through automated teller machines (ATMs) situated close to the conflict zones in Syria, Iran or Iraq. This threat specifically concerns the Turkish regions bordering these countries. The analysis of ATM withdrawals over the last two years from these specific regions shows that said withdrawals were rather limited, both in volume and in value. Importantly, no evidence such as TFTRs[19]/TFARs[20] linked to these transactions suggests that these rather small amounts were linked to TF or FTFs.

5.3. International organisations and other terrorist actors

As mentioned beforehand, larger organisations need important funds to maintain infrastructure, propaganda and operational capacities on top of the funds needed to perpetrate terrorist attacks. Therefore, they need to raise funds either through criminal activities performed by their organisation (e.g. trafficking, extortion, etc.) or from outside through wealthy terrorism sponsors. The main threat posed by terrorist organisations and their sponsors consists of the misuse of Luxembourg's financial centre to channel larger funds from or to international terrorist organisations established in regions particularly impacted by terrorism. This threatens the more sophisticated subsectors of the financial sector, mainly private banking and the investment sector.

[19] TFTRs is a Terrorist financing transaction report.

[20] TFAR is a Terrorist financing activity report.

The VRA assessed that terrorist organisations operate in regions characterised by an active terrorist threat or from terrorist safe havens. In order to determine Luxembourg's exposure and that of its financial centre, the following steps were followed:

1) **Selection of jurisdictions relevant for the purpose of this analysis**. As said beforehand, in relation to the threat posed by ISIL, the selected jurisdictions are situated in both the Middle East and Northern Africa and Sub Saharan regions.
2) **Analysis of financial flows.** Out of the 50 selected jurisdictions, it appears that for most of the studied flows[21], the three jurisdictions ranking first in terms of value account for more than half of the analysed flows.
3) **Analysis of Mutual Evaluation Reports** from those jurisdictions with whom Luxembourg maintains larger financial flows.
4) **Analysis of other variables and flows** (e.g. Luxembourg's demographic structure, imports and exports, residents of those jurisdictions registered with Luxembourg's company - or beneficial owner registry, and Luxembourg non-profit organisations (NPOs) carrying out development and humanitarian projects in those jurisdictions).

Links to those jurisdictions are twofold. First, from an economic perspective, Luxembourg maintains bilateral relationships with some of these jurisdictions, including active promotion of Luxembourg as a business destination. Secondly, with regard to development cooperation and humanitarian aid, Luxembourg has signed Indicative Cooperation Programmes with its partner countries, which are general cooperation framework agreements to provide development aid.

Thus, it can be concluded that the analysed flows occur within intended and bilateral frameworks. The volume and nature of these flows did not reveal a material threat to Luxembourg's financial centre with respect to TF.

[21] Studied financial flows for the purpose of this report were, amongst others, bank deposits, loans granted to residents of the selected jurisdictions, correspondent banking, investments in Luxembourg banks by residents from those jurisdictions, investments issued by residents of those jurisdictions held by Luxembourg residents, foreign direct investments from Luxembourg to those jurisdictions (and *vice versa*), wire transfers.

Insight n°1

The table below provides a summary of the financial requirements of the different types of terrorism actors and highlights, for each actor type, which TF stages are likely to occur in Luxembourg.

Table 1: Summary of previous sections

Terrorist activity in…	Type of terrorism actor	Financial requirements	TF stage likely to take place in Luxembourg
…EU and UK	Lone actors and small terrorist organisations	Small financial requirements (<€10 000); mostly funded from legitimate activities	Raising (through legitimate income) Moving (by abusing services of Luxembourg's financial centre commensurate with their lower TF needs) Using (by executing a hypothetical attack)
	FTFs	Small financial requirements (<€10 000); FTFs are either self-funded or via recruitment networks	
…Third countries, especially the world regions most impacted by ISIL	International terrorist organisations and other terrorist actors[22]	Very high financial requirements	Raising (Luxembourg residents' donations to NPOs carrying out development and humanitarian projects abroad) Moving (by sending funds to international terrorist organisations by abusing Luxembourg's services commensurate with their higher financial needs)
	"Corporate" terrorist groups		Moving (by abusing services of Luxembourg's financial centre commensurate with their higher TF needs)

[22] Except for "corporate" terrorist groups.

6. ASSESSING TERRORIST FINANCING VULNERABLE SECTORS

6.1. Sectoral vulnerabilities

The main TF risks for Luxembourg emanate from the threat that terrorists, terrorist organisations and their financiers might exploit the vulnerabilities of certain sectors essentially for moving funds. The 2020 NRA contains a detailed study of the ML/TF vulnerabilities of the various sectors whose professionals are subject to the Law of 12 November 2004 (2004 AML/CFT Law). The following subsections provide a detailed view of the vulnerable (sub-) sectors.

Traditional banking products offered by **retail and business banking** (e.g. debit/credit cards, wire transfers, ATM withdrawals) make them vulnerable to TF by lone actors, small terrorist cells or FTFs that could misuse them to move funds cross-border. It is interesting to point out that Luxembourg retail banking activities are focused on a local clientele. According to a recent survey conducted by the CSSF and the Luxembourg Bankers' Association (ABBL) on the retail banking activity[23,24], the majority of assets and liabilities are held by national residents (88%). Retail and business banks filed the highest number of STRs: 22 TFARs in 2020 (8 in 2019) and 4 TFTRs in 2020 (14 in 2019)[25].

Private banking's exposure to TF is driven by their size, international exposure, and nature of their clients (i.e. prevalence of big and potentially more sophisticated accounts). The financial threshold for entering into a business relationship and the close links with its clients (e.g. products are designed for a long-term relationship, use of relationship managers) make private banking unattractive to actors with low financial requirements. However, wealthy terrorism sponsors might enter into asset or wealth management agreements with Luxembourg private banks with a view to harbouring their assets even though the assets or wealth under management in Luxembourg might not be related directly to TF.

Similar to retail and business banking, the products and activities offered by the **MVTS's sector** allow easy access to fast and convenient cross-border transactions. This makes the sector vulnerable to being abused by FTFs, lone actors and small cells operating within the EU. The size and volume of transactions of Luxembourg's PI and EMI sub-sectors are large, while only a few agents/e-money distributors of PIs/EMIs, established in other EU Member States, operate in Luxembourg[26].

As for the private banking subsector, the **investment sector's** exposure to TF appears more relevant for wealthy terrorism sponsors outside the EU than for lone actors or small terrorist cells operating within the EU. This is particularly true for the wealth and asset management subsector which typically caters to high net worth individuals. However, there is limited evidence that the investment sector is misused for TF purposes, as reflected by the very low number of TFARs and TFTRs filed. Notwithstanding this and similar to private banking, the sector's size is considered as a vulnerability factor.

[23] ABBL and CSSF, *Retail banking survey,* 2020 (link).

[24] Clients classified as retail banking clients for the purposes of this study were private individuals, professionals (self-employed, liberal professionals etc.) and legal entities (generally small companies etc.), excluding corporate and private banking clients.

[25] CRF, *Activity report 2020* (link).

[26] Whereas in 2020 21 PIs/EMIs handle 2.5 billion inflow transactions worth €118.1 billion and 1.5 billion outflow transactions worth €95 billion, Luxembourg counts 22 Luxembourg-based agents and 3 e-money distributors acting on behalf of PIs/EMIs established in another EU Member State that handle 4 million inflow transactions worth €232.7 million and 253 932 outflow transactions worth €294 million. The large customer base of Luxembourg licensed PIs/EMIs accounts for those important figures (in terms of number and volume).

It is important to highlight that within the private banking and investment sector, investment decisions may be performed on a discretionary basis. This means that investment decisions are taken by the professional and not by the client. Consequently, it is unlikely that funds are "moved" or "used" for TF purposes in the private banking and investment sector. In a similar vein, it is crucial to differentiate between the investments performed by the professional for the client, and the client's usage of those returns. Funds held within retail and business banking and by MVTS providers are not subject to a discretionary management. Instead, clients can use the basic financial services to move funds and perform various transactions.

Globally, **NPOs carrying out development and humanitarian projects abroad** are exposed at two key points of their operations: through the donations they receive and the destination of their funds.

- Regarding donations, organisations linked to terrorists or terrorist groups have been known to create false appeals to raise money. In most cases, donations are made by the public in the belief that the money will be used to fund genuine charitable activities. However, occasionally the donors are aware of the true destination of the funds and use the humanitarian cover to avoid raising suspicion. No such cases have yet been identified in Luxembourg, but the vulnerability exists;
- Regarding the destination of the funds, money may be paid by NPOs active in projects abroad (with or without DNGO status[27]) to individual terrorists or terrorist groups, deliberately or inadvertently. As above, no such cases have yet been identified in Luxembourg, but the vulnerability exists.

Although the globally observed typologies have not been detected in relation to Luxembourg NPOs developing projects abroad, this sub-sector remains highly vulnerable in view of the geography of their activities.

6.2. Cross-sectoral vulnerabilities

Globally, **cash** is the most frequently observed mode of transportation for criminal purposes, including for TF. Yet there is no known evidence for the collection of cash for TF purposes in Luxembourg (e.g. donations being solicited by shady TF-related NPO's or individuals acting on their behalf). Notwithstanding this, the TF risks resulting from the use of cash in Luxembourg should still be considered by public and private entities. The number of border cash declarations received by the *Administration des Douanes et Accises* (ADA) has remained relatively stable over the past four years and, in 2020, the total value represented 0.02% of the total value of cash declared to customs authorities across the EU in the same year[28]. As mentioned beforehand, Turkey is considered a major transit hub for FTFs given its geographical location. The analysis of ATM withdrawals linked to accounts held with Luxembourg financial institutions near the Syrian, Iranian and Iraqi border shows that those were rather limited. Importantly, no evidence, such as TFTRs/TFARs linked to these transactions, was found to suggest that these amounts were linked to TF or FTFs.

[27] NPOs with a goal of international cooperation and development (DNGOs) are specifically defined and accredited by the Ministry of Foreign and European Affairs (MoFA).

[28] European Commission, *Customs union - facts and figures,* 2020 (link).

Social media and crowdfunding activities are vulnerable to TF misuse. While the overall crowdfunding market in Luxembourg is limited (the market volume was estimated between €1 million and €5 million in 2015[29]), a significant part of the global crowdfunding uses payment methods such as bank transfers, credit/debit cards and internet payment services[30]. Luxembourg banks, PIs and EMIs offer such services to other professionals abroad. With respect to crowdfunding platforms, Luxembourg counts one institution offering payment solutions to crowdfunding platforms. Although the share of clients of this institution involved in crowdfunding is very limited, this could present a potential vulnerability.

Although the 2019 European Supranational risk assessment recognised the risks of **virtual assets** being misused to finance terrorism as emerging[31], a recent report from Europol states that the number of cases involving virtual assets for TF remains limited[32]. As of 31 December 2021, Luxembourg counts six registered virtual asset service providers (VASPs). Six TFTRs/TFARs related to virtual assets or VASPs were reported to the CRF in 2020 and 29 in 2021. There is no evidence that Luxembourg VASPs are significantly exposed to TF.

According to a recent report published by the Royal United Services Institute, it appears that new technologies (e.g. social media and crowdfunding, virtual assets) have not played a predominant role in the financing of most European terrorist attacks (i.e. those performed by lone actors and small cells). In most cases, attack-related items had been previously owned by the attacker or had been procured using cash or other common banking payment methods[33]. Terrorist groups have globally been observed to use virtual assets, donation-based crowdfunding, social media and payment services providers, especially in the "raising" and "moving" stages[34]. Overall the report states that new technologies have been added to, rather than replaced, traditional financing methods[35].

[29] Cambridge Centre for Alternative Finance, *The 2nd European Alternative Finance Industry Report*, 2016.
[30] Asia/Pacific Group on Money Laundering and Middle East and North Africa FATF, *Social Media and Terrorist Financing*, 2019.
[31] European Commission, *Supranational Risk Assessment,* July 2019 (link).
[32] Europol, *Europol Spotlight: Cryptocurrencies: tracing the evolution of criminal finances,* 2022 (link)
[33] Royal United Services Institute, *Bit by Bit,* 2022 (link).
[34] Royal United Services Institute, *Bit by Bit,* 2022 (link).
[35] Royal United Services Institute, *Bit by Bit,* 2022 (link).

Insight n°2

The conclusions drawn in the previous sections are condensed in the following table:

Table 2: Linking the different TF actors with their TF needs, TF stages that may potentially take place in Europe (including Luxembourg) and vulnerable sectors

	TF activities linked to FTFs, lone actors and small terrorist cells	**TF activities linked to international terrorist organisations, State sponsors, terrorist safe havens and corporate terrorist groups**
TF needs	Small financial requirements	Very high financial requirements
TF stages that may potentially take place in Europe	Raising, moving and using[36]	Raising and moving
TF vulnerable sectors	Retail banking, business banking, and MVTS	Private banking, investment sector, and NPOs carrying development and humanitarian projects abroad
TF cross-sector vulnerabilities[37]	Cash, *social media, crowd funding,* and *virtual assets*	*Social media, crowdfunding,* and *virtual assets*

7. MITIGATING FACTOR ANALYSIS

The potential medium or higher TF risks identified are mitigated by counter-measures, called mitigating factors.

As described in the 2020 NRA, Luxembourg's **mitigating factors' framework** relies on five pillars, namely i) national strategy and coordination, ii) prevention and supervision, iii) detection, iv) prosecution, investigation and asset recovery, and v) international cooperation. Furthermore, these mitigating factors are based **on a comprehensive legal AML/CFT framework** consistent with the FATF Recommendations and the fourth and fifth EU anti-money laundering directives.

[36] Note that FTFs would raise funds in Luxembourg and rather move them abroad with the intention to use them in third countries. Lone actors and small terrorist cells would typically use the funds in Luxembourg/the EU.

[37] Available data does not allow to allocate vulnerabilities stemming from social media, crowdfunding and virtual assets to a specific type of terrorist actor. For this reason, and by adopting a conservative approach, those cross-sectoral vulnerabilities are considered relevant for all the different types of terrorist actors studied in Table 3.

7.1. Prevention and supervision

Luxembourg understands the specific nature of the TF risks described above and developed appropriate and specific CFT measures in addition to the general AML/CFT framework. As determined beforehand, the banking (and more precisely retail and business banking, as well as private banking), the investment and the MVTS sectors and Luxembourg NPOs carrying out development and humanitarian projects abroad are considered vulnerable to being misused for TF purposes. Consequently, those sectors are analysed in the subsequent paragraphs.

The banking, investment and MVTS sectors apply similar mitigating measures. They all fall within the scope of the 2004 AML/CFT Law and the Law of 19 December 2020 (2020 Sanctions Implementation Law) and must, therefore, comply with preventive provisions regarding ML, TF and targeted financial sanctions (TFS). As outlined in the vulnerabilities' section, those sectors are primarily exposed through their clients and transactions.

With regard to the risks stemming from the customer, the banking and investment sector and MVTS providers perform customer due diligence at on-boarding and throughout the business relationship. This includes, amongst others, name screening without delay of their clients' database against TFS.

With respect to the risks stemming from transactions, those professionals have put in place transaction monitoring systems. In particular banks, PIs and EMIs providing e-commerce services have adopted performant automated transaction monitoring systems that allow them to group transaction reports, identify trends and share in a structured way appropriate high quality reports (TFTRs and TFARs) with the CRF. This allows for a faster and more effective cooperation.

In addition, payment service providers (such as professionals from the banking and MVTS sector) must comply with the obligations arising from Regulation (EU) 2015/847 on information accompanying transfers of funds, which are especially useful to counter TF risks related to lone actors and small terrorist cells within the EU.

PIs and EMIs licensed in another EU Member State and that operate in Luxembourg through **agents/e-money distributors** must appoint a central contact in Luxembourg as soon as they meet specific criteria[38]. This contact point must ensure adequate communication and information reporting in accordance with the provisions set out in Title III and IV of the law of 10 November 2009 on payment services. These contact points must also provide the CSSF and the competent authorities in the Home Member State with information on request in order to facilitate supervision.

The **CSSF** is the authority responsible for the supervision of several types of professionals with respect to AML/CFT, including the banking, the investment and MVTS sectors. It performs TF-related controls at market entry and during its on-going supervision. As part of the market entry controls, the CSSF conducts fit and proper assessments.

[38] In accordance with the European Supervisory Authorities's joint Regulatory Technical Standards on the criteria for determining the circumstances in which the appointment of a central contact point pursuant to Article 45 (9) of Directive (EU) 2015/849 is appropriate and the functions of the central contact point, PIs and EMIs established in other Member States and offering their services through agents or e-money distributors shall appoint a central contact point amongst others where they operates through 10 or more agents/e-money distributors, or the total volume of transactions carried out exceeds €3 million etc.

Furthermore, the CSSF assesses the envisaged activity and the purpose of establishing a business in Luxembourg in order to detect whether the professional could be used or abused for TF activities. Besides, TF specific controls are included in the CSSF's AML/CFT on-site control plan.

To date, the CSSF has detected no violation of TFS for TF, and consequently, no sanction has been issued on this subject. Nonetheless, on a number of occasions, the CSSF has identified general breaches in relation to requirements on transaction monitoring, enhanced due diligence measures and "name matching" controls, which ultimately may include a TFS-related component. Since this is an important subject for the CSSF, these deficiencies have been sanctioned or, if of minor importance, administrative measures have been issued, requiring for adequate remediation by the professional.

Even though NPOs are not professionals subject to the 2004 AML/CFT Law, some **Luxembourg NPOs engaged in development and humanitarian projects abroad** have implemented specific CFT controls, for example, name screening systems such as WorldCheck, to evaluate risk levels of their partners and beneficiaries of funds, but this applies to a small share of entities. Furthermore, similar to local NPOs, Luxembourg NPOs that engage in development and humanitarian projects abroad benefit from preventive measures put in place by the service providers they use, for example, on transaction monitoring systems put in place by banks when performing bank wire transfers.

Finally, Luxembourg NPO may apply to obtain DNGO status by MoFA in order to receive subsidies to co-fund their projects abroad. In this case, MoFA performs checks on DNGOs in order to ensure the appropriate use of government funds. In September 2021, the MoFA published and updated the general conditions document in order to include CFT aspects. Even though the MoFA controls do not target TF specifically, the absence of MoFA controls expose NPOs carrying out development and humanitarian projects abroad without DNGO status at a higher TF risk.

7.2. Detection

The CRF plays a key role in the **detection** of TF activities through the receipt and analysis of STRs and the dissemination of its strategic and operational analysis products, allowing the identification of suspicions of terrorism and TF by reporting entities and providing support for investigations.

Between 2015 and 2020, the CRF received 1 891 TF reports with 454 reports relating to 2020 and 444 to 2019. The number of TF reports significantly increased from 2017 on. The large customer base of some Luxembourg PIs/EMIs explains this surge. These institutions, which operate online, have numerous customers in all EU Member States. STRs not having a direct link with Luxembourg are systematically shared with the concerned Member State or third country financial intelligence unit.

The high number of reports concerning other countries shows that the private sector is aware of the risks associated with their customers. The CRF strives to ensure the best possible international cooperation with its counterparts in order to guarantee the effectiveness of the system.

7.3. Prosecution and conviction

All **potential TF and related terrorism cases are systematically investigated** at a very early stage even when there is only the slightest suspicion with the aim of preventing these crimes from occurring.

As previously said, there are no known Islamic terrorist cells operating in Luxembourg and only a few FTFs have left Luxembourg to join ISIL in Syria. Although closely monitored, none have returned yet. The first **prosecution** and **conviction** took place in Luxembourg in 2021 for acts related to Islamic-related terrorism. Luxembourg does consider the low prosecution and conviction rates as a result of its successful early investigation strategy.

7.4. International cooperation

Given Luxembourg's open economy and the financial centre, Luxembourg authorities **provide prompt international cooperation** in the field of TF. This includes CRF cooperation with foreign financial intelligence units, police cooperation through Europol and Interpol, judicial authorities' cooperation through mutual legal assistance requests and supervisor's cooperation with their international counterparts.

8. RESIDUAL RISK

The inherent TF risks are being reduced as a result of the above-mentioned mitigating measures. The table below provides the outcomes of the mitigating factors and residual risk analysis for the sectors and subsectors analysed in detail in the report.

Table 3: Summary of sector and subsector mitigating factors and residual risk assessment

Sector	Subsector	Inherent TF risk		Residual TF risk
Banks	Private banking	**Medium**		**Low**
	Retail and business banks	**High**		**Medium**
Investment sector	Wealth and asset managers	**Medium**		**Low**
	Collective investments	**Medium**	*Impact of mitigating factors*	**Low**
Money value and transfer services	Payment Institutions E-money institutions Agents and e-money distributors acting on behalf of PI/EMIs established in other European Member States	**High**		**Medium**
NPOs carrying out development and humanitarian projects abroad	NPOs (*Associations sans but lucratif* (ASBLs) and *fondations*) carrying out development and humanitarian projects abroad	**High**		**High**

To conclude, the following sections elaborate on Luxembourg's TF residual risk at the three stages of TF: raising, moving and using funds.

Table 4: Conclusion

	Raising	Moving	Using
Retail and business banking	Small cells, lone actors and FTFs may raise legitimate funds such as salaries, social benefits, non-paid-off customer loans, overdrafts	Basic financial services (e.g. wire transfers/ ATM withdrawals) might be misused to move funds intended for TF purposes to small cells, lone actors and FTFs	Small cells, lone actors and FTFs may use funds to commit terrorist acts
Private banking **Investment sector**	Relevant for wealthy terrorism sponsors outside the EU	Discretionary asset management is not suitable for moving funds for TF purposes. Funds managed by the asset manager under a discretionary contract are inaccessible to the customer. Generated returns that are no longer subject to discretionary management may be transferred to terrorists or terrorist organisations	Not applicable as long as the funds are under discretionary management This does not exclude the investment sector from performing (enhanced) due diligence on investment projects in regions impacted by terrorism and companies operating in such regions
MVTS	Small cells, lone actors and FTFs may abuse MVTS providers to raise funds for TF purposes (including payments related to crowdfunding services)	MVTS might be misused to move funds intended for TF purposes to small cells, lone actors and FTFs	Small cells, lone actors and FTFs may use funds to commit terrorist acts
NPOs carrying out development and humanitarian projects abroad	NPOs may raise funds (advertently or inadvertently) for TF purposes	Some high-risk jurisdictions have limited access to the international correspondent banking systems and some NPOs carrying out development and humanitarian projects abroad may be tempted to use informal or non-regulated channels (e.g. Hawala or other service providers) to transfer funds to those jurisdictions No evidence of Hawala or other service providers operating in Luxembourg	Not applicable, except for NPOs raising funds advertently for TF purposes

APPENDIX A. LIST OF TABLES

A.1. List of tables

Table 1: Summary of previous sections 10
Table 2: Linking the different TF actors with their TF needs, TF stages that may potentially take place in Europe (including Luxembourg) and vulnerable sectors 14
Table 3: Summary of sector and subsector mitigating factors and residual risk assessment 17
Table 4: Conclusion 18

APPENDIX B. ACCRONYMS

B.1. List of acronyms

Acronym	Definition
ABBL	The Luxembourg Banker's Association
ADA	*Administration des Douanes et Accises*
AML/CFT	Anti-money laundering and countering terrorist financing
ASBL	*Association sans but lucratif*
ATM	Automated teller machines
CRF	*Cellule de Renseignement Financier*
CSSF	*Commission de Surveillance du Secteur Financier*
DNGO	Non-governmental organisation for development
EMI	E-money institution
EU	European Union
FATF	Financial Action Task Force
FTF	Foreign Terrorist Fighter
GTI 2020	Global terrorism index 2020
ISIL	Islamic State of Iraq and the Levant
ML	Money laundering
MoFA	Ministry of Foreign and European Affairs
MVTS	Money value or transfer services
NPO	Non-profit organisation
PI	Payment institution
STR	Suspicious transaction report
TF	Terrorist financing
TFAR	Terrorist financing activity report
TFS	Targeted financial sanction
TFTR	Terrorist financing transaction report
UK	United Kingdom
VASP	Virtual asset service providers
VRA	Vertical risk assessment