AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Guideline :

Terrorist financing awareness guide for the private sector (Financial Institutions and Designated Non-Financial Professionals and Businesses)

and

Anti-money laundering, terrorist and proliferation financing

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

I. Introduction

The purpose of this guideline is to assist Financial Institutions (FI) and Designated Non-Financial Professionals Businesses (DNFPBs) ("Supervised Entities") in raising awareness and understanding risks associated with terrorist financing and applicable AML/CFT obligations. The guidance contained in this document should be applied risk-based and proportionate, considering the size, nature, and complexity of the business of each financial institution and DNFPB.

This Guideline considers standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices, and red flag indicators identified by the FATF. These are not exhaustive and do not restrict supervised entities' actions to fulfil their legal obligations within the current legal and regulatory framework. In light of their nature, size, and complexity, supervised entities should assess how best to fulfil their legal obligations.

The scope of this Guideline is purely informative. The only legally binding documents are the legislative and regulatory texts governing the anti-money laundering, counter-terrorism and proliferation financing, and corruption framework in Monaco. All obligations and their details are therefore not addressed herein: solely applying the measures presented in this Guideline does not ensure that the institution fully complies with current legal obligations.

The relevant provisions in force in the Principality relating to the financing of terrorism are set out in Sovereign Order 15.320 of 8 April 2002 on the suppression of the financing of terrorism and in Article 391-7 of the Criminal Code.

It was subsequently improved by the provisions of Law no. 1.362 of 2009, as amended, on the fight against money laundering, terrorist financing and corruption.

Compliance with current legal and regulatory obligations, based on the specific risks it faces, is the responsibility of each obliged entity. This guideline takes into account the regulations in force as of **September 30, 2023**.

II. Context

Terrorist attacks cause casualties, loss of property and a climate of fear, threatening the safety of states and the security of citizens.

Their number has increased in recent years, and they can occur on a small or large scale and be carried out collectively or by individuals acting alone.

The development of terrorist activities can be facilitated by online media designed to fuel radicalisation and home-grown extremism, leading to attacks using improvised explosive devices, firearms, knives or vehicles.

In many countries, the political landscape is marked by a significant increase in radical ideas, which constitutes a threat from the point of view of individuals prepared to commit attacks. (See Global Terrorism Index https://www.economicsandpeace.org/reports/)

Extremist nationalist movements can also pose a major threat, jeopardising the stability of nations and democratic processes. Groups that plan to carry out terrorist acts or that actually do so need funding.

Under Law no. 1.362 as amended, Supervised Entities are obliged to report unusual or suspicious transactions, movements of capital or illicit assets, which may be investigated even before the underlying criminal offence has been detected.

Although the risk of a terrorist attack in the Principality can currently be considered low, it cannot be ruled out that funds intended for use in such a venture could transit through the financial centre.

III. Terrorist Financing risks

In 2021, the Principality of Monaco conducted a detailed Terrorism Financing (TF) Risk Assessment to determine the level and types of risks that the country faces in this regard. In 2023, this understanding was updated when the Strategic Committee led and coordinated the 2023 Terrorism Financing National Risk Assessment (the 2023 TF NRA).

The 2023 TF NRA aimed to complement the 2021 TF risk analysis, to deepen and to expand Monaco's risk understanding on TF. It was based on the analysis of a wide set of data and information sources and benefitted from input by all relevant stakeholders in Monaco through numerous workshops and meetings.

The 2023 TF NRA considers the specific factors that characterise terrorism financing threats and vulnerabilities in the Monegasque context by examining different risk scenarios and allocating those risk scenarios under each of the three principal terrorism financing methods – collection, movement, and use. Monaco's low domestic terrorism risk, its status as sophisticated and high-profile international financial centre focused on private wealth management, and its geographic location in the middle of Europe were the main perspectives through which the assessment was conducted.

Having identified and assessed the main risk scenarios that the country faced, combined with an evaluation of the risk mitigating measures in place, the assessment found that overall there is a medium-low country risk that financial systems in Monaco are being misused for TF purposes.

Breaking this rating down into the individual risk scenarios that were analysed in the assessment, the risk profile can be summarized as follows:

Risk Scenario	Inherent Risk	Mitigating Measures	Residual Rating
Risk Scenario 1 – Funds Transfers to/from high-risk jurisdictions	Medium-high	Substantial	Medium-low
Risk Scenario 2 – Customers or Beneficial Owners of Monegasque FIs or DNFBPs are terrorism financers	High	Substantial	Medium-High
Risk Scenario 3 – Beneficial Ownership by Terrorism Financers of Monegasque FIs or DNFBPs	Low	Moderate	Low
Risk Scenario 4 – Monegasque legal entities are beneficially owned or controlled by terrorism financers	Medium-High	Strong	Medium-Low
Risk Scenario 5 – Use of Cash or Travellers Cheques to move value for terrorism related purposes	Medium-Low	Substantial	Low
Risk Scenario 6 – Correspondent Banking	Low	Strong	Low
Risk Scenario 7 – Donations by Monegasque to foreign NPOs or Use of Monegasque NPOs for terrorism financing purposes	Low	Strong	Low
Risk Scenario 8 – Use of High Value Commodities to Move Value for Terrorism Related Purposes	Medium-High	Moderate	Medium-High
Risk Scenario 9 – Carrying out a Terrorist Attack	Medium-Low	Strong	Low
Risk Scenario 10 – Maintaining Terrorist Networks or Infrastructure on Monegasque Territory	Low	Strong	Low

Monaco's inherent risks relating to the use of funds in Monaco for terrorism purposes are low. Monaco's risk exposure in relation to the collection and movement of terrorism related funds is however slightly higher than had previously been assumed and is determined to be medium-low in both categories.

Funding Method	Monaco's Exposure
1 – Collecting terrorism related funds in Monaco	Medium-low
2 – Moving terrorism related funds through Monaco	Medium-High
3 - Using terrorism related funds in Monaco	Low
OVERALL	Medium-Low

Monaco's geographic proximity to countries with terrorism activity coupled with its political stability, its vibrant high-end luxury market, and its globally connected financial markets could make the country attractive for terrorist organizations and networks to collect, invest or otherwise move funds and value through the system. Monaco's status as international financial centre exposes the country to a heightened risk of being misused to channel terrorism related funds through its financial system.

IV. What is terrorist financing (TF)?

1) Terrorists' Financing needs

Terrorist organisations take different forms (large state-like organisations, small, decentralised groups or autonomous networks), and attacks can be carried out by individuals who draw their inspiration from radicalised environments, or who have themselves been radicalised.

These terrorists, who generally act alone, need to be able to finance their activities, which can pose difficulties when it comes to defining observable indicators.

'Lone wolf' terrorists fall into two categories:

- Those inspired by radical ideologies propagated by terrorist organisations, often based abroad,
- Those who become radicalised as a result of a triggering factor specific to the environment in which they live (opposition to the government, frequenting places of worship or associations, for example).

These terrorists seek to control the entire process, from financing to carrying out the attack.
Terrorists' funding needs reflect this diversity and vary greatly from one structure to another. This may be not only to fund specific terrorist operations, but also to cover the wider operational costs of setting up and maintaining a terrorist organisation, and to create the environment in which it can operate.

The perpetrators of terrorist acts therefore need to find funds to finance their activities. Whether it's to cover day-to-day expenses such as food and accommodation, travel, training and equipment, or to carry out the acts themselves, they need money.

These funds may come from third parties (financiers or supporters) or from the assets or income of the terrorists themselves and may be of legal or illegal origin. Terrorists may finance their activities from legitimate sources (salaries or income, savings, credit cards, for example), illicit sources (criminal activities, financiers or agents), or receive financial support from third parties (family, friends, public services and administrations, charities, etc.).

The direct cost of organising individual acts is modest compared to the damage they can cause.

However, maintaining a terrorist network, or even a smaller cell, requires a large amount of resources for

recruitment, planning and purchasing. Maintaining international terrorist networks and promoting their objectives over the long term requires significant infrastructure and logistics. Terrorist organisations therefore need large amounts of money to create and maintain an infrastructure of international support, fuel their ideology through propaganda activities and finance the ostensibly lawful activities needed to give themselves an appearance of legitimacy.

2) Terrorist Financing process

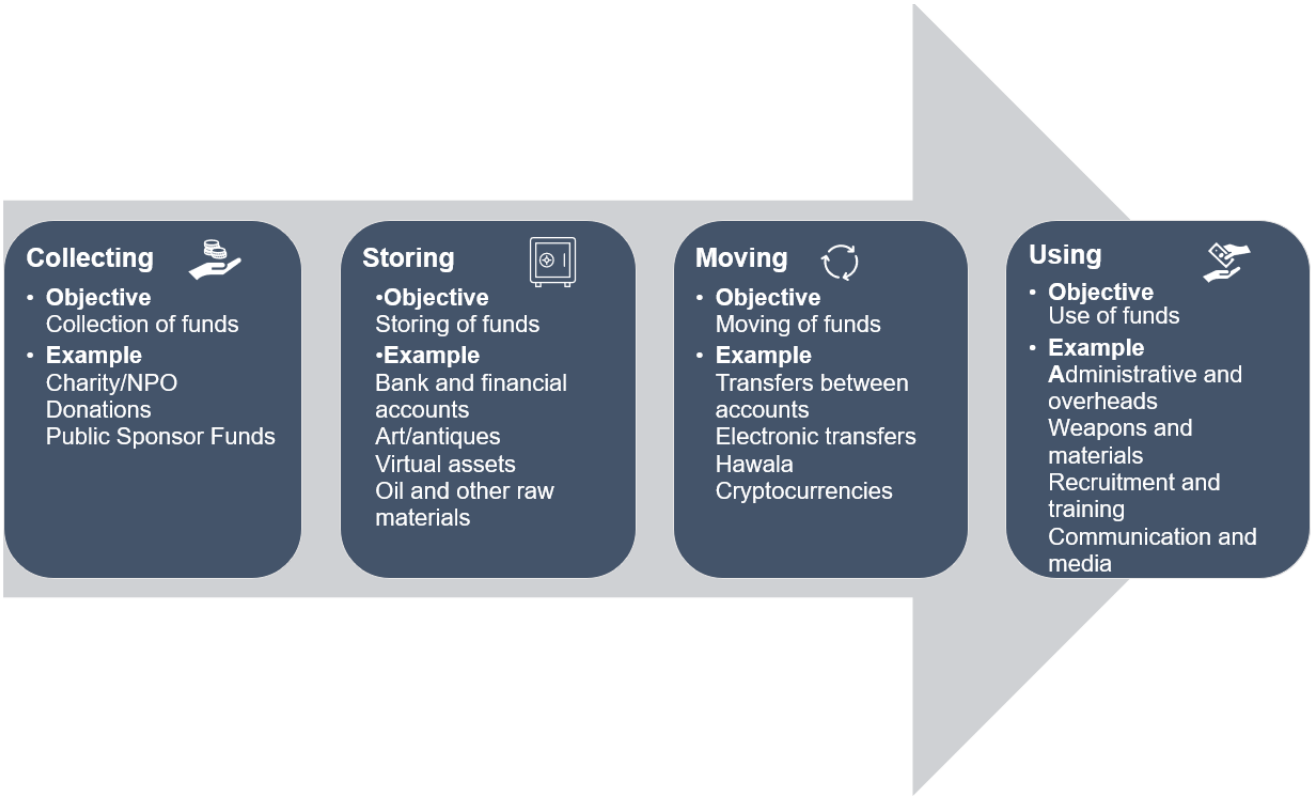
This process consists of :

- Collect funds from various sources to be used to support the terrorist organisation
- Store funds until their use can be determined and planned
- Transmit funds as and when required
- Use the funds as necessary to contribute to the objectives of the terrorist organisation

TF process	
Collection	The types of financial support used to finance terrorism generally include direct donations from individuals and organisations, charities and non-profit organisations, and criminal activities. Direct donations: The sources of financial support belonging to this category often consist of funds of legal origin, of any amount, donated by individuals, legal entities, non-profit organisations (NPOs) or companies and, in some cases, foreign countries. Funds subsequently used for terrorist purposes may also originate from salaries, wages, social benefits, personal donations or company profits. Individuals can make donations from income or grants received by themselves or their families; they can also raise funds on a small scale from members of their community (neighbours, places of worship, etc.), or launch broader appeals via the Internet, social networks or participatory funding sites. Donors may not know what their funds will ultimately be used for. Charities and not-for-profit organisations (NPOs): While the vast majority of charities carry out legitimate and important work, the FATF noted that this sector could be particularly vulnerable to diversion for terrorist financing purposes. Appeals by charities, non-profit organisations and similar entities for donations to help "those in need" are particularly attractive to those involved in terrorist financing. They provide an opportunity to raise funds from a wide range of potential donors among the general public, due to the emotional nature of appeals to help vulnerable or suffering populations, and many governments also encourage this practice by allowing taxpayers to deduct all or part of their donations from their income. Although charities also manage cash, it is more difficult to trace the origin, movement and use of funds. Some of them have an international presence and work with other groups located close to conflict zones in which terrorist organisations may be active, or be in contact with them. Criminal activities: Some terrorist organisations use separate criminal networks to raise funds. Drug trafficking, fraud, cybercrime and white-collar crime are among the illicit activities commonly used to finance terrorism. In the case of foreign fighters and violent

	extremists of national origin, the misappropriation of public aid/benefit programmes and the use of fictitious reimbursements have been identified as fund raising typologies. Terrorist organisations based in large geographical areas can seize financial assets and natural resources belonging to a State in the territory they control. Non-monetary assets and resources (antiquities, crude oil, natural gas, ores, precious metals and stones) will need to be converted into cash or some other form in which they can readily be used, for example by means of illicit transactions with third partiesor on the black market. It is possible that these black markets operate to a large extent outside the territories or countries where the terrorists are based.
Storage	Funds can be stored in numerous ways: ❖ Bank accounts ❖ Prepaid cards ❖ Storage of large volumes of cash ❖ High-value goods such as oil, art/antiques, agricultural products, precious metals and stones and second-hand vehicles ❖ Virtual Assets
Movement	Known mechanisms for channelling funds include the following: ❖ The banking and financial sector ❖ The money remittance sector, for example authorised money service businesses (MSBs) ❖ Informal value transfer systems (e.g. hawala) and bureaux de change ❖ The clandestine transport of cash ❖ The smuggling of high-value goods such as oil, art/antiques, agricultural produce, precious metals and stones, and second-hand vehicles. ❖ Virtual Assets
Use	The funds can be used for terrorist purposes in a number of ways, for example: ❖ Terrorist organisations: weapons and equipment, administrative procedures and overheads, media and messaging, recruitment and training, financial assistance for human resources, family financial support, communications equipment, means of transport, corruption, accommodation, planning and preparation of missions to commit terrorist acts ❖ Foreign fighters: travel, passport/visa costs, outdoor/survival equipment, weapons and combat training ❖ Lone terrorists and small terrorist cells: weapons and equipment, vehicles (purchased or leased), minimum financial resources for food and shelter, means of communication, transport and any other purchases required for terrorist plots. Some of these uses relate to day-to-day expenses that are difficult to link to terrorism.

The diagram below illustrates the four stages of the terrorist financing process.



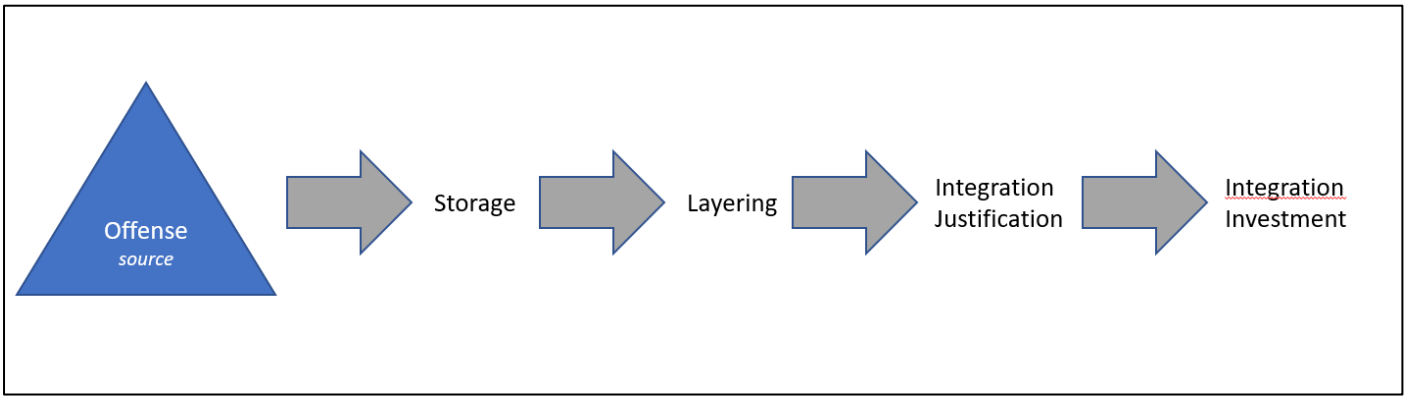
V. Money laundering versus terrorist financing

1) Similarities and differences between ML and TF

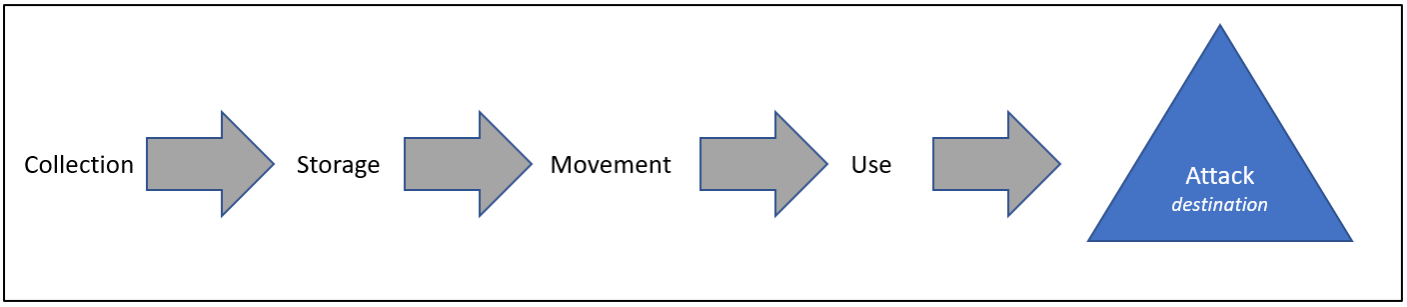
The offences of money laundering and terrorist financing can be committed in conjunction with each other, for example when the funds made available to terrorist organizations are funds that have previously been laundered. However, although the two activities have common characteristics and typologies, their timing and the purpose of their operations differ.

In the case of money laundering, the emphasis is on the origin of the funds, whereas with terrorist financing, the emphasis is on their use. As a result, while in both cases secrecy and mobility are imperatives, in the case of terrorist financing it is generally not necessary to go through a concealment or integration-justification phase before reaching the stage where the funds will be used.

Money laundering is a circular enterprise: it involves collecting the proceeds of criminal activities, then processing them before returning them to the perpetrators of these activities.



Terrorist financing, on the other hand, is an essentially linear process involving the collection of funds and assets, whether of legitimate or illicit origin, their storage and transport to the point where they are to be used.



Self-laundering occurs when the criminal himself facilitates the laundering of his funds. This pattern can

also be seen in the financing of terrorism by individual terrorists. In fact, when economic funding can be obtained on the initiative of an individual himself (through his work, through criminal activities or by any other means), it is possible for him to store the funds to build up a financial base from which to prepare an attack, then to channel the money or investments to places where they can be used, and finally to use them to carry out the attack. In this case, the entire process is carried out by one and the same person.

It is important to bear in mind that while there are similarities between money laundering and terrorist financing (in terms of methodology, mobility, the need for secrecy, etc.), the objectives, behaviour and sources of terrorist financing are different.

2) Detection of unusual transactions linked to terrorist financing

Detection focuses primarily on unusual transactions indicating a possibility of money laundering or terrorist financing. "Unusual" is defined as a transaction that differs from the prevailing norms in a particular sector or that deviates from an individual's habits, given their profile, normal activities or declared income. Any deviation from normal or expected conduct may indicate a risk. The greater the deviation and the more unusual the situations, the greater the risk of money laundering or terrorist financing. It is therefore essential to carry out a more detailed assessment.

Unusual transactions linked to the financing of terrorism often have certain characteristics which make it possible to conceal and justify the movement of funds and/or the use of the money collected:

- Fundraising involving charities and/or not-for-profit organizations (e.g. anonymous donations)
- Use of well-known money laundering methods (movements) or procedures (investment)
- Use of funds to acquire services and/or products that do not correspond to the profile of the person concerned or the organization concerned
- Movement of funds (or other assets) to or from conflict zones or neighboring regions

VI. AMSF Expectations

Considering the unique characteristics of terrorist financing and associated risks, FI and DNFBPs are expected to have:

AMSF Expectation related to compliance to CFT Obligations by FI and DNFBPs

- Adequate Business Risk Assessment that corresponds to the size, nature, and business profile of the entity and which distinguishes between money laundering and terrorist financing risk;
- Include TF in Internal Policies and Procedures;
- Specific FT Training and awareness raising;
- Adequate Customer Risk Assessment;
- Checks when onboarding clients and ongoing monitoring of Customer Relationships;
- Adequate transaction monitoring systems that enable entities to identify and report suspicious transactions in a timely manner;
- Adequate systems and controls to manage TF Risks;
- Statistics on TF specific alerts, specific examinations and STRs.

VII. ANNEXES

ANNEX I : Trends in terrorism and terrorist financing

Every year, the publications office of the European Union publishes the Europol (European Union Agency for Law Enforcement Cooperation) European Union Terrorism Situation and Trend Report (the TESAT report). The most recent version was published in December 2023 and is available on Europol's website.

The TESAT report recognises that in recent years the terrorism landscape in the EU has evolved and the threat now goes well beyond that posed by Islamic extremist groups. The report identifies the following broad categories of terrorism practised by groups who are active in the EU member states and who pose a direct threat to their stability and security;

Jihadist Terrorism is defined as 'a violent sub-current of Salafism, a revivalist Sunni Muslim movement that rejects democracy and elected parliaments, arguing that human legislation is at variance with God's status as sole lawgiver. Jihadists aim to create an Islamic state governed exclusively by Islamic law (shari'a), as interpreted by them'. Major representatives of jihadist groups are the al-Qaeda network and the self-proclaimed Islamic State (IS) terrorist group.

Right Wing Terrorism is defined as 'the use of terrorist violence by right-wing extremists. Violent right-wing extremist individuals and groups use, incite, threaten, legitimise or support violence and hatred to further their political or ideological goals. They seek to change the entire political, social and economic system into an authoritarian model and, in doing so, reject the democratic order and values as well as fundamental rights. Violent right-wing extremist ideologies are centred on exclusionary nationalism, racism, xenophobia and/or related intolerance. In addition, violent right-wing extremist ideologies feed on a variety of hateful sub-cultures, commonly fighting back against diversity in society and equal rights of minorities. A core concept in right-wing extremism is supremacism or the idea that a certain group of people sharing a common element (nation, race, culture, etc.) is superior to all other. Seeing themselves in a supreme position, the particular group considers it to be their natural right to dominate the rest of the population.

Left wing terrorism is practised by groups who seek to trigger a violent revolution against the political, social and economic system of a state, in order to introduce socialism and eventually establish a communist and classless society. Their ideology is often Marxist-Leninist.

Anarchist terrorism is a term used to describe violent acts committed by groups or individuals promoting the absence of authority as a societal model. Anarchists pursue a revolutionary, anti-capitalist and anti-authoritarian agenda.

Ethno-nationalist and separatist terrorist groups are motivated by nationalism, ethnicity and/or religion. Separatist groups seek to carve out a state for themselves from a larger country or annex territory from one country to that of another. Left-wing or right-wing ideological elements are not uncommon in these types of groups.

The TESAT report also recognises the existence of numerous other groups and ideologies that hold extreme views whose actions are disruptive to society, such as those practised by environmental and animal rights groups; these actions could, if taken to the extreme, be classed as terrorist acts.

The TESAT report highlights the following developments in the financing of terrorist groups of all types in 2022 and 2023;

Funds to finance terrorist activities across the whole ideological spectrum are attained through various ways, including legal business structures, the collection of donations, membership fees and criminal activities.

The use of legal business structures by terrorists and violent extremists to raise funds continued to be observed in 2022. Left-wing, anarchist, right-wing, ethno-nationalist and separatist extremists and terrorists also use legal business structures to collect and launder funds used for terrorist financing, including bars, coffee shops, gas stations, kiosks, restaurants and pubs.
The sale of merchandise, videos, publications and tickets for events (for example concerts), including on e-commerce platforms is another way to raise funds. In particular, social media platforms provide terrorists and violent extremists with low-cost advertising and sales channels for a broader target group inside and outside the scene.

Donations are an integral part of terrorist financing for all terrorist phenomena. Donations are collected in person at events (for example at affiliated concerts) and places of gathering, but also via bank transfers.

The Islamic State receives donations from family members and supporters, and the money is remitted to foreign terrorist fighters (FTFs) and their families who are in Syrian prison camps. Although most funds collected by jihadists are directed to conflict zones, investigations also indicate that the money is used for

radicalisation and recruitment efforts among the jihadist communities in the EU.

Donations are also collected under the guise of humanitarian aid by jihadist terrorists in Europe and are then mostly sent to conflict zones in countries such as Afghanistan, Iraq, Somalia and Syria, transiting neighbouring countries, usually Türkiye and Lebanon. The Partiya Karkerên Kurdistanê (Kurdistan Workers' Party, PKK) collects large amounts of money within the EU through their annual international fundraising campaign 'kampanya'.

Terrorist and violent extremist organisations adhering to various ideologies raise funds through membership fees or through crowdfunding campaigns, which are often advertised on social media platforms and increasingly on cloud-based mobile applications.

Across the entire ideological spectrum, funds used to finance terrorism are also attained through criminal activities. The most reported offences are drug trafficking, extortion, kidnapping, robbery, theft, human trafficking and document fraud. Economic and financial crimes are also significant sources of funds, and include tax fraud, tax evasion, social benefit fraud, and the illegal use of public funds.

The most common ways to transfer funds remain the traditional banking system, money transfer services, and informal value transfer systems (IVTS) such as hawala. However, the traditional banking system is less used in the Member States where control mechanisms and risk profiling are strict or new anti-money laundering legislation has been introduced. Online payment platforms are also reported as a way of raising and transferring funds.

The ways in which jihadist terrorist organisations are moving funds is evolving however. More layers are used to cover the transactions, which are taking place globally. For instance, cryptocurrencies are paid to an account in one country where they are withdrawn, the amount is divided and sent via hawala to other countries and further transferred via money transfer services. When sent to conflict zones, cash is usually withdrawn from money transfer offices by money mules who deliver it to the final beneficiary.

Terrorist organisations increasingly use digital currencies and virtual assets service providers (VASPs), as these provide a higher level of anonymity for donors and recipients. However, the use of digital currencies remains marginal among the means of terrorist financing. As regards jihadism, IS and al-Qaeda and their affiliates appear to have stepped up the use of VAs, especially cryptocurrencies, for fundraising and the movement of funds in recent years, possibly as a result of an increased knowledge of VAs among members of jihadist terrorist groups. Right-wing extremists also resort to funding platforms operating with

cryptocurrencies.

Foreign Terrorist Fighters (FTFs) and lone actors : historically the phenomenon of radicalised individuals from foreign states heading for conflict zones to participate in a war for what they perceived as an ideological purpose was almost entirely restricted to Jihadist groups. Recent intelligence however indicates a rise in the number of individuals from Right Wing terrorist groups who have expressed an interest or intention to travel to Ukraine to participate in the Russian war of aggression, on both sides of the battleground.

In November 2022, the European Parliament proposed to include several pro-Russian groups such as the Russian paramilitary organisation known as 'the Wagner Group', the 141st Special Motorised Regiment, known as the 'Kadyrovites', as well as other Russian-funded armed groups, militias and proxies, on the EU's terrorist list; some intelligence suggests that certain individuals with extremist views may have tried to join these groups. Other information suggests that the majority of the European right-wing extremists support Ukraine. Calls to join the ultra-nationalist Ukrainian Azov battalion have been circulating in the right-wing extremist scene.

A significant number of FTFs from a range of ideologies who have gained experience of combat and have survived their experiences, have left the battlefields and returned to their home countries. The principal security risk concerning FTFs is those individuals who have returned to their home countries and remain radicalised, and who seek to carry out terrorist attacks at home or in neighbouring countries.

Whilst the threat from FTFs engaged in fighting in Iraq and Syria has diminished, FTFs are increasingly travelling to other combat areas such as Ukraine and North and West Africa. From a TF perspective, FTFs provide support to terrorist groups in theatre by travelling with funds and material and receive support to continue fighting or to return home. Self-funding by individuals and funding by recruitment/facilitation networks are assessed as the two most common methods used to raise funds for FTFs.

Individuals often use funds from legitimate sources (e.g., employment income, social assistance, family support, bank loans) to finance their travel to the conflict zone. In some cases, investigations have revealed that small businesses were intentionally established and used to generate revenue that supported FTF travel. Some jurisdictions have also noted the sudden sale of assets including personal belongings and assets purchased on credit just prior to the FTFs planned travel.

In this respect, there are some similarities between FTFs and small terrorist cells and lone actors. The

activities of lone terrorists can be very difficult to spot, although analysis carried out after attacks show that it is still possible to identify indicators and identify small financial traces.

The lone terrorist will seek to control the entire process himself, the aim most of the time being to acquire the resources to carry out a terrorist act. When the tactical option chosen involves small-scale attacks, this is not generally evident in the data to be analysed and/or verified. On the other hand, when the attack is more complex and the level of resources used is greater, certain indicators can be identified.

A lone terrorist may need to undertake complex efforts, such as tax or VAT fraud, to accumulate funds in order to lend or provide premises where preparations can take place. The fraud will then generally be committed by a declared company that will act as a screen. This company may also be used to acquire goods (e.g. fertilisers or other forms of chemical products, or products that should attract attention or even be subject to a declaration obligation on the part of retailers). One or more companies may be used to further conceal the routing of goods to the scene of the attack, and to conceal possible intentions after the attack, or to cause confusion, as well as to disguise the possible involvement of a larger number of people.

ANNEX II : Terrorist financing indicators

In order to assist in the identification of unusual transactions, these general characteristics have been broken down into several groups of indicators, as follows:

- Indicators relating to individuals
- Indicators relating to businesses
- Indicators relating to charities and non-profit organisations
- Cryptocurrency indicators

The presence of an indicator does not establish with certainty the existence of an illegal activity. In fact, correct and duly justified explanations for the presence of these indicators may emerge by carrying out open source checks and questioning the customer. Furthermore, not all indicators are equally significant or reliable in every situation when it comes to uncovering money laundering or terrorist financing activities.

It is therefore rare that a specific isolated indicator can immediately give rise to a reasonable suspicion that a terrorist financing operation is involved. This means that it is necessary to gather additional and conclusive evidence/information of possible terrorist financing (e.g. evidence reported by verified external sources such as lists communicated by national authorities, United Nations list, etc.).

An illustrative (but not exhaustive) list of Terrorist Financing Indicators

Indicators relating to individuals

Indicators Associated with Funding and support	Financial activity ❖ Misuse of social benefits or questionable tax refund claims ❖ Financial support (or payments for expenses or goods) from an unexpected or undetermined source ❖ Transfer of funds to or from conflict zones or neighbouring regions ❖ ATM operations in conflict zones or neighbouring regions ❖ Movements of funds unrelated to employment relationships or other financial arrangements ❖ Bank card limit reached or close to its limit following cash withdrawals ❖ Accumulation of loans from various lenders over a short period, with the possibility of non-repayment ❖ Payments for travel to and from conflict zones or neighbouring regions ❖ Large or frequent donations to charities with links to conflict zones or neighbouring regions ❖ Payments to media outlets or bookshops that help to propagate radical, extremist or violent ideas (e.g. for propaganda purposes, to set up a printing business, manufacture brochures, flags, etc.) ❖ Changes in monetary practices, such as sudden recourse to less transparent financial instruments ❖ Use of transfers to or from high-risk countries or between persons located in the same country or territory, the amounts of which are below the reporting thresholds in order to avoid detection, or which have no commercial purpose ❖ Power of attorney over a third party's bank account ❖ Loans granted to individuals for non-commercial purposes (generally without repayment) ❖ Monetary donations to known extremist entities ❖ Payments made using encrypted money transfer applications (e.g. mobile messaging applications) ❖ Accumulation of funds from various sources in a single account and transfer to a single receiving account (e.g. possible actor), within the country or abroad ❖ Loans, lines of credit and/or credit card borrowing without repayment ❖ Use of one or more shell companies ❖ Loans, lines of credit or credit card borrowing without repayment ❖ Purchase or sale of high-value goods (e.g. cultural goods) from conflict zones or neighbouring regions ❖ Buying or selling counterfeit goods ❖ Numerous requests for loans

	❖ Deposits of cash in volumes excessive in relation to declared or known sources of cash income, particularly in personal accounts ❖ Deposit transactions carried out in a place that is geographically very distant from the place where the accounts or owners are domiciled ❖ Unexpected cash amounts kept on business premises or at home ❖ Rapid transfer or disbursement of funds following cash deposits <u>Personal behavior</u> ❖ Radicalisation (e.g. adopting a name associated with extremist or fundamentalist groups or movements, a sudden change in lifestyle or behaviour, wearing traditional religious clothing, etc.) ❖ Expression of extremist political or religious views ❖ Criticism of the government or its policies in relation to terrorism-related issues, propagation of radical, extremist or violent ideas (e.g. via social networks) ❖ Travel to and from conflict zones or neighbouring regions ❖ Inclusion on a sanctions list ❖ Inclusion on the client list of a tax preparer/accountant involved in illicit refund schemes
Indicators Associated with Organizers and agents	<u>Financial activity</u> ❖ Transfer of funds to or from conflict zones or neighbouring regions ❖ ATM operations in conflict zones or neighbouring regions ❖ Movements of funds unrelated to employment relationships or other financial arrangements ❖ Bank card limit reached or close to its limit following cash withdrawals ❖ Payments for travel to and from conflict zones or neighbouring regions ❖ Coverage of costs associated with acquiring specific skills (piloting licences, firearms permits, driving licences for large vehicles/vessels, etc.). ❖ Payments to media outlets or bookshops that help to propagate radical, extremist or violent ideas (e.g. for propaganda purposes, to set up a printing business, manufacture brochures, flags, etc.) ❖ Payments corresponding to the rental of "meeting" spaces without any economic advantage or other logical explanation

- Loans or funds received from a third party with no commercial purpose (generally without repayment)
- Payments made using encrypted money transfer applications (e.g. mobile messaging applications)
- Loans, lines of credit and/or credit card borrowing without repayment
- Property transactions financed from unknown sources
- Purchase or sale of high-value goods (e.g. cultural goods) from conflict zones
- Loans from conflict zones or neighbouring regions
- Deposits of cash in volumes excessive in relation to declared or known sources of cash income, particularly in personal accounts
- Small cash deposits spread over several bank accounts held or controlled by the same person, with an unexplained increase in the total amount of deposits
- Deposit transactions carried out in a place that is geographically very distant from the place where the accounts or owners are domiciled
- Tax refunds that appear to be fictitious
- Unexpected cash amounts kept on business premises or at home
- Cash withdrawals in high-risk countries and neighbouring regions
- Rapid transfer or disbursement of funds following cash deposits
- Suspicious or fictitious repayments to recurring customers (may indicate that a company has transferred funds to one or more persons belonging to a terrorist cell)
- Use of transfers to or from high-risk countries or between persons located in these countries, for amounts below the reporting thresholds in order to avoid detection
- Purchase of dual-use goods (e.g. electronic products, chemical substances, weapons, training materials, survival kits, maps, GPS, smartphones equipped with PGP encryption/decryption software), etc.)

<u>Personal behavior</u>

- Radicalisation (e.g. adopting a name associated with extremist or fundamentalist groups or movements, a sudden change in lifestyle or behaviour, wearing traditional religious clothing, etc.)

	❖ Isolation from family, friends, work and society in general ❖ Expression of extremist political or religious views ❖ Criticism of the government or its policies in relation to terrorism-related issues, propagation of radical, extremist or violent ideas (e.g. via social networks) ❖ Travel to and from conflict zones or neighbouring regions ❖ Inclusion on a sanctions list ❖ Inclusion on the client list of a tax preparer/accountant involved in illicit refund schemes
Indicators Associated with Actors and performers	<u>Financial activity</u> ❖ Significant change in tax filing habits (e.g. late filing) ❖ Misuse of social benefits or questionable tax refund claims ❖ Financial support (or payments for expenses and goods) from an unexpected or undetermined source ❖ Large or frequent cash transactions in proportion to income level (e.g. support from unrelated third parties) ❖ Transfer of funds to or from conflict zones or neighbouring regions ❖ ATM transactions in conflict zones or neighbouring regions ❖ Bank card limit reached or close to its limit following cash withdrawals ❖ Accumulation of loans from various lenders over a short period, with the possibility of non-repayment ❖ Payments for travel to and from conflict zones or neighbouring regions ❖ Coverage of costs associated with acquiring specific skills (e.g. piloting licences, firearms licences, large vehicle/vessel licences, etc.). ❖ Loans or funds received from a third party with no commercial purpose (generally without repayment) ❖ Loans, lines of credit or credit card borrowing without repayment ❖ Loans from conflict zones or neighbouring regions ❖ Numerous loan applications ❖ Payments made using encrypted money transfer applications (e.g. mobile messaging applications) ❖ Payments to extremist media or bookshops ❖ Buying or selling counterfeit goods ❖ Cash deposits from unknown sources

	❖ Deposits of cash in volumes excessive in relation to declared or known sources of cash income, particularly in personal accounts ❖ Deposit transactions carried out in a place that is geographically very distant from the place where the accounts or owners are domiciled ❖ Unexpected cash amounts kept on business premises or at home ❖ Cash withdrawals in high-risk countries and neighbouring regions ❖ Rapid transfer or disbursement of funds following cash deposits ❖ Purchase of dual-use goods (e.g. electronic products, chemical substances, weapons, training materials, survival kits, maps, GPS, smartphones equipped with PGP encryption/decryption software, etc.) <u>Personal behavior</u> ❖ Radicalisation (e.g. adopting a name associated with extremist or fundamentalist groups or movements, a sudden change in lifestyle or behaviour, wearing traditional religious clothing, etc.). ❖ Isolation from family, friends, the workplace and society in general ❖ Expression of extremist political or religious views ❖ Criticism of the government or its policies in relation to terrorism-related issues, propagation of radical, extremist or violent ideas (e.g. via social networks) ❖ Travel to and from conflict zones or neighbouring regions ❖ Inclusion on a sanctions list ❖ Inclusion on the client list of a tax preparer/accountant involved in illicit refund schemes

Indicators relating to businesses	
Indicators Associated with unusual transactions and parties	❖ Transactions (shipments, transfers, money transfers, transport of funds, etc.) with parties located in conflict zones or neighbouring regions ❖ Transfers of funds without going through regulated financial institutions (hawala and other informal money transfer systems, for example) ❖ Money transfers using encrypted money transfer applications (e.g. mobile messaging applications) ❖ Transactions with unusual lenders ❖ Suspicious or fictitious repayments to recurring customers (may indicate that a company has transferred funds to one or more persons belonging to a terrorist cell) ❖ Risky goods such as high-value items and dual-use goods in large quantities ❖ Inconsistency between the pattern and size of transactions and the company's reported activity
Indicators Associated with unusual capital movements	❖ Numerous capital movements to and from commercial accounts with no apparent economic purpose ❖ Absence of documents concerning the purpose, origin or destination of funds ❖ Rapid transfer or disbursement of funds following cash deposits ❖ Cash withdrawals in high-risk countries and neighbouring regions ❖ Cash deposits in excess of declared or known sources of cash income ❖ Deposit transactions carried out in a place that is geographically very distant from the place where the accounts or owners are domiciled ❖ Indicators relating to other forms of fraud (credit cards, loans, etc.), such as suspicious or unusual loan applications or credit card payments ❖ Unexpected cash amounts kept on business premises or at home
Indicators Associated with business activities	❖ Purchase or storage of assets unrelated to the company's business (for example, a printing works buying gas masks, encrypted telephones, camping equipment, fertilisers) ❖ Purchase or storage of excessive quantities of restricted or listed dual-use products (radioactive materials, chemicals, explosives, etc.) ❖ Unexplained shortage of stocks of dual-use goods ❖ Sale of restricted or listed dual-use items to unknown or unauthorised buyers

	❖ Cash deposits and other assets in excessive amounts unrelated to turnover or indebtedness ❖ Company assets used by unknown or unidentified persons or entities for no consideration
Indicators Associated with unusual expenses	❖ Payments for travel to and from conflict zones or neighbouring regions for the benefit of another person ❖ Large or frequent donations to charities with links to conflict zones or neighbouring regions ❖ Company purchases of assets that cannot be located or verified ❖ Invoices for advertising, publishing and printing services unrelated to the company's activities (presumably for propaganda purposes, to set up a printing business, produce brochures, flags, etc.). ❖ Goods or expenses of a private nature paid for by the business and which are apparently not used by the owner of the business

Indicators relating to charitable and non-profit organizations (NPOs)	
Indicators Associated with unusual transactions and parties	❖ Donations received from a state that finances terrorism or from foreign entities located in or near a conflict zone, particularly in the absence of a clear link or supporting documents ❖ Accumulation of large and insufficiently justified donations, especially if they are made mainly in cash ❖ Use of funds to finance expenditure unrelated to the activity of a non-profit organisation ❖ Money transfers to countries and territories that have no connection with the activities of a charitable or not-for-profit organisation ❖ Actual expenditure incurred for the purchase of goods that do not correspond to the wording on the invoices or dispatch notes ❖ An entity that presents itself as a charity but operates unregistered in order to avoid scrutiny by regulators ❖ Executives, key members of staff or major donors who have previously worked for other charities that have been the subject of suspicion or sanctions ❖ Directors, key members of staff or major donors who are the subject of negative information from freely accessible sources ❖ Associated foreign entities, representatives or employees who are the subject of negative information from freely available sources ❖ Transfer of funds or other assets to entities located/operating in or near conflict zones, in particular if no activities or programmes have been reported in these zones ❖ Association of directors, trustees, managers, key staff or representatives of a charitable or not-for-profit organisation with organisations or individuals with links to terrorism. ❖ Propagation, distribution, publication on the Internet or other media, of extremist ideologies or documents that glorify them

Indicators relating to virtual assets	
Indicators Associated with unusual transactions and parties	❖ Use of cash to purchase Virtual Assets ❖ Frequent, small value VA transactions to the same recipient or address or linked recipients and addresses ❖ Frequent, small value VA transactions to the same recipient or address or linked recipients and addresses using different VAs and VASPs ❖ Individual sends transactions to the same address from different addresses or wallets ❖ Use of Peer to Peer VA providers ❖ Use of VASPs in remote locations close to conflict zones ❖ Transactions to addresses advertised on social media or web sites as linked to extremist groups ❖ Transfers to NPOs providing services in conflict zones or those affected by natural phenomena ❖ Use of so-called 'Privacy Coins' to make donations or carry out transactions ❖ Out of character transactions, or lack of explanation for carrying out transactions ❖ Round amount transactions ❖ Lack of interest in cost of coins and pricing fluctuations ❖ Use of VA ATMs to carry out transactions despite higher fees ❖ Use of VASPs, with weak anti-money laundering checks and policy (such as Know-Your-Customer) - a company such as Chainalysis, which provides blockchain data and analysis, draws up a list of such exchanges for its clients ❖ Multiple rapid transactions between multiple VASPs or platforms without a clearly related purpose, which may indicate attempts to break through the chain of custody on the respective blockchains or to further disguise the transaction
Indicators Associated with Darknet transactions	❖ A user often receives funds from, or deposits funds into, darknet wallet addresses which accumulate large values ❖ A significant percentage of the deposits made by a user on an exchange originate from darknet market places ❖ A significant percentage of the withdrawals of a user of an exchange result in transactions with darknet market places

VIII. Case studies

Virtual assets

As awareness and acceptance of Virtual Assets increases, incidences of them being used for illicit purposes also increases. The use of Virtual Assets as a mechanism to store and transmit funds is now integrated into the modus operandi of many large scale money laundering groups, and the same is increasingly true of terrorist financiers. Investigations in the USA, India, Indonesia and the Philippines reveal that jihadist terrorist groups have been soliciting donations through various forms of virtual assets since at least 2015; although the sums themselves were not large they were used to successfully carry out a number of significant terrorist attacks resulting in loss of life and damage to property.

In 2018, a page appeared on a website affiliated with Islamic state encouraging sympathisers to send bitcoin to an address that was detailed on the web page, encouraging followers to 'fund the Islamic struggle without leaving a trace'. The website was taken down by the US FBI. In 2019, Hamas engaged in a cryptocurrency donation campaign that led in 2020 to the seizure by the US Government of several websites and 150 cryptocurrency accounts linked to the armed wing of Hamas, the Izz al Din al Qassam Brigades. The U.S. Department of Justice (DOJ) charged two foreign nationals for money laundering crimes related to their involvement in converting cryptocurrency into other forms of value. DOJ also prosecuted an individual for concealing material support to Hamas, including through Bitcoin.

Investigations in the US in 2023 revealed that Qassam Brigades had used Binance, a cryptocurrency exchange, to facilitate cryptocurrency transactions since as early as 2019. In 2021, the U.S. cryptocurrency exchange platform Coinbase identified Hamas as one of several terrorist groups involved in cryptocurrency fundraising. Israeli authorities reportedly seized dozens of cryptocurrency addresses linked to Hamas, Palestinian Islamic Jihad (PIJ), and other terrorist groups between 2021 and 2023. In April 2023, the Qassam Brigades announced it would stop accepting Bitcoin donations, cautioning that donors could be targeted.

In October 2023 open source reporting stated that cryptocurrency wallets connected to Hamas received about $41 million between 2020 and 2023 and that wallets connected to PIJ received as much as $93 million over a similar period.

Investigations suggest that Virtual Asset donations to terrorist groups are usually solicited via social media campaigns or on web pages, with the web pages often given the appearance of belonging to a charity or some other body purporting to provide humanitarian aid to persons in conflict zones or areas affected by natural disasters such as earthquakes and floods. Donations are also made via transfers through large Virtual Asset Service Providers such as Binance and Coinbase.

IX. GLOSSARY

Terms	Definition
Terrorism	The United Nations defines terrorism as "criminal acts which, for political purposes, are intended or calculated to provoke a state of terror in the public, a group of persons or particular individuals, and which are unjustifiable under any circumstances and whatever the grounds of a political, philosophical, ideological, racial, ethnic, religious or other nature which may be invoked to justify them".
Terrorist Financing	Terrorist financing is the act, by any means whatsoever, directly or indirectly, illegally and deliberately, of providing, gathering or managing funds, with the intention of seeing them used or knowing that they will be used, in whole or in part, either: ❖ by a terrorist; ❖ by a terrorist organization; ❖ with a view to committing one or more acts of terrorism. The offense is committed even if the funds were not actually used to commit or attempt to commit one or more acts of terrorism, nor are they linked to one or more specific acts of terrorism.
Funds	the term and expression "funds" have the meaning given to them by article 1 of the United Nations International Convention for the Suppression of the Financing of Terrorism adopted in New York on December 9, 1999[1].
Governmental or public installation	the term and expression "governmental or public installation" have the meaning given to them by article 1 of the United Nations International Convention for the Suppression of the Financing of Terrorism adopted in New York on December 9, 1999.
Products	the term and expression "products" have the meaning given to them by article 1 of the United Nations International Convention for the Suppression of the Financing of Terrorism adopted in New York on December 9, 1999.

[1] Convention made enforceable by Ordinance n° 15.319 du 8 avril 2002.