



Technical Paper

**Operational guidance for law enforcement agencies and prosecutors: identifying
and investigating terrorist financing**

Prepared by:
Professor Nicholas Ryder
Council of Europe Expert

Date: November, 2025

This technical paper is prepared as part of the Council of Europe's Action against corruption, money laundering and terrorist financing in Bosnia and Herzegovina (BiH). The overarching objective of this project is to augment trust in the rule of law and democracy by undertaking comprehensive efforts to combat economic crimes and adhere to internationally recognized standards.

The action supports the capacity of the institutions in preventing and combating economic crime by focusing on enhanced measures and capacities for corruption prevention; improving anti-money laundering/countering the financing of terrorism supervision and enforcement of preventive measures; and strengthening capacities to effectively apply seizures and confiscations of illegal assets.

For further information please contact:

Economic Crime Cooperation Division
DG I, Council of Europe

E-mail: contact.econcrime@coe.int
www.coe.int/econcrime
www.coe.int

Disclaimer:

This technical paper is prepared by the Council of Europe's Economic Crime and Cooperation Division.

The views and opinions presented herein are those of the experts and should not be taken as to reflect the official position of the Council of Europe.



Table of contents

Acronyms	4
Executive Summary	5
1. Introduction	7
2. Chapter Two – International standards and country specific context	8
3. Chapter Three – Concepts and definitions	10
4. Chapter Four - Patterns and red flags in terrorist financing	12
5. Chapter Five - Circumstances that may indicate terrorist financing	21
6. Chapter Six - Sources of information for identifying and investigating terrorist financing	41
7. Chapter Seven - Best practices and patterns in identifying terrorist financing	53
8. Chapter Eight - Summary and key recommendations	59
9. Appendixes	61
Reference List	74



Acronyms

Anti-Money Laundering	AML
Bosnia and Herzegovina	BiH
Counter Terrorist Financing	CTF
Criminal Code of Republika Srpska	RS
Financial Action Task Force	FATF
Financial Intelligence Unit	FIU
Islamic State of Iraq and Levante's	ISIL
Law Enforcement Agencies	LEAs
Money Laundering	ML
Money or Value Transfer Services	MVTS
Non-profit organizations	NPOs
Organised Criminal Gangs	OCGs
Terrorist Financing	TF



Executive Summary

This document provides operational guidance for law enforcement agencies (LEAs) and prosecutors to identify and investigate terrorist financing. It sets out a practical framework that clarifies the range of circumstances, red-flag indicators and information sources that reveal terrorist financing activity. The guidelines align with international best practices and relevant FATF standards and emphasise timely, coordinated action across financial and criminal intelligence functions.

Purpose and scope

The guidelines are designed to be actionable and practitioner-focused, offering:

- Red-flag indicators and realistic detection scenarios;
- A structured catalogue of information sources, including Financial Intelligence Unit (FIU) data, financial institutions, customs and tax authorities, international cooperation mechanisms, open-source intelligence, and vulnerable sectors;
- Practical steps for converting intelligence into investigative leads and prosecutable cases.

Core approach and principles

The guidance promotes a dual-track approach that integrates financial intelligence and criminal intelligence. Financial data alone may miss small-value transfers; criminal intelligence techniques can identify individuals providing assets, informal transfer channels, and other forms of material support. The document encourages cooperation, information-sharing and joint operational planning as prerequisites for effective disruption.

Key operational elements

Red-flag indicators and scenarios:

- Evidence based scenario indicators to help frontline officers and analysts recognise suspicious patterns early.

Information sources:

- A prioritised catalogue of sources (FIU reports, bank records, customs/tax data, international requests, and open-source material) mapped to likely indicators.

Investigative toolkit:

- A recommended mix of financial analysis, surveillance, undercover operations, communications analysis, and controlled operational techniques to follow leads and preserve evidence.

Prosecutorial integration:

- Guidance on evidence standards, case packaging, and legal considerations to convert investigations into successful prosecutions.



Intelligence integration and cooperation

The guidelines emphasise that only a coordinated combination of financial intelligence and criminal intelligence, supported by formal cooperation mechanisms, will reliably detect and disrupt terrorist financing schemes. They recommend establishing joint task forces, shared analytic products, and routine liaison with FIUs, financial supervisors and international partners to close information gaps.

Compliance with FATF standards

The guidance references FATF expectations that competent authorities be empowered to use a wide range of investigative techniques. This includes undercover operations, intercepting communications, access to computer systems, and controlled deliveries. Aligning operational practice with these standards is presented as essential for both effectiveness and international cooperation.

Conclusion and next steps

The adoption of these draft guidelines will strengthen early detection, improve investigative outcomes, and enhance prosecutorial success by standardising indicators, broadening the intelligence toolkit, and institutionalising cross-agency cooperation.



1. Introduction

This document presents draft guidelines for law enforcement agencies (LEAs) and prosecutors on identifying and investigating terrorist financing. Its purpose is to provide a practical, operational framework that clarifies the range of circumstances, indicators and information sources that can reveal terrorist financing activity. The guidelines seek to incorporate international best practices and relevant Financial Action Task Force (FATF) standards and will set out red-flag indicators and realistic scenarios in which terrorist financing may be detected. They will provide a structured catalogue of information sources, including FIU data, financial institutions, customs and tax authorities, international cooperation mechanisms, open-source intelligence and sectors vulnerable to terrorist financing misuse.

Guidelines aimed at supporting law enforcement agencies and prosecutors in identifying terrorist financing at an early stage **should include** not only financial intelligence tools but also criminal intelligence tools necessary to identify individuals providing assets to support terrorist groups, as well as asset transfer channels and the provision of other material support. It should be noted that criminal intelligence methods can also be effective in identifying small amounts of assets used for terrorist financing, as well as the covert nature of this criminal activity. Only a combination of criminal and financial intelligence tools, as well as close cooperation between agencies responsible for criminal and financial intelligence, is the key to success in identifying, investigating and disrupting terrorist financing schemes and channels.

It should be noted that FATF Recommendation No. 31. Powers of law enforcement and investigative authorities requires countries to ensure that competent authorities conducting investigations can use a wide range of investigative techniques appropriate for investigating money laundering, related predicate offences, and terrorist financing. These techniques include undercover operations, communications interception, access to computer systems, and controlled deliveries, which can be considered classic tools of criminal intelligence.



2. Chapter Two – International standards and country specific context

Criminalising terrorist financing removes the financial lifelines that allow groups and individuals to plan, recruit, buy weapons, and undertake terrorist attacks. It provides LEAs and prosecutors clear powers to investigate, arrest, prosecute, and seize assets, and it strengthens cooperation with the private sector to identify and stop suspicious flows of money. National criminal laws must be aligned with the UN Convention on Terrorist Financing (1999) and FATF Recommendations. Clear criminal penalties and active enforcement deter potential financiers making it harder for terrorist groups to sustain long-term planning and operations.

In relation to terrorist financing the FATF endorsed Fifth Round Mutual Evaluation Report for BiH, conducted by MONEYVAL in February 2024, concluded that authorities classify terrorist financing risk as medium, but weaknesses in legal definitions and case outcomes do not match that assessment. Some terrorist financing cases have been identified and investigated. LEAs have demonstrated investigative skills, but not all available information sources are used to detect the crime, and interpretations of the terrorist financing offence are inconsistent across agencies. The judiciary in particular shows a limited understanding, which undermines law-enforcement motivation and persistence in pursuing cases that diverge from the established interpretation. A recently developed national counter-terrorism strategy and action plan now incorporate lessons and results from TF investigations.¹

Item A.5. The preventive security measures provided for in the Counter-Terrorism Strategy clearly indicate that:

As part of the preventive action in the jurisdiction of security agencies, this priority measure includes the strengthening of capacities and procedures for the gathering, analysis and exchange of operational, intelligence, financial-intelligence and criminal-intelligence data and knowledge about activities that indicate the planning or commission of criminal offences of terrorism and offences related to terrorism.

C. RESPONSE / REACTION to potential terrorist attacks and remediation of their consequences

Coordination at all levels will be strengthened in terms of the exchange of operational, intelligence and police data.

D. IMPROVEMENT of procedures of investigation, criminal prosecution, penitentiary and post-penal treatment in cases of terrorism and related criminal offences:

Procedures for the collection, analysis, cooperation and exchange of operational, intelligence, financial-intelligence, information-security and criminal-intelligence data on activities that

¹ Moneyval (2024).



indicate the planning or commission of criminal offences of terrorism and related criminal offences will also be improved.

The country introduced new mechanisms to speed up implementation of terrorist financing and proliferation financing targeted financial sanctions (TFS), but these mechanisms do not impose direct penalties for non-compliance and for much of the review period a cohesive TFS framework was absent. Only one designation was made under UN Security Council Resolution 1373, and the wider designation process is subject to delays with unclear links between terrorism/terrorist financing investigations and consideration for designation. Implementation of TFS obligations is uneven across sectors.²

² Ibid.



3. Chapter Three – Concepts and definitions

3.1 Introduction

This section defines terrorist financing and distinguishes it from money laundering and other financial crimes; it outlines how international instruments and standard-setters characterise financing as the provision, collection or solicitation of assets intended to support terrorism.

3.2 Terrorist Financing

Terrorist financing is defined by the International Convention for the Suppression of the Financing of Terrorism as including ‘assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form.’³ The Convention states that a person commits the criminal offence of terrorist financing ‘if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out’.⁴ The FATF Glossary defines terrorist financing as the financing of terrorist acts, and of terrorists and terrorist organisations.⁵

The concept is deliberately broad: it includes tangible and intangible property, legal instruments, and services. Criminal liability arises where a person unlawfully and wilfully provides or collects such funds or resources to be used, in full or in part, to carry out terrorist activity. Examples include:

- A donor gives cash to a charity that secretly diverts funds to buy weapons for a terror group
- An individual rents a safe house where recruits are radicalised and attack plans are drafted
- A business owner invoices fake consultancy work to move “clean” profits to a terrorist cell
- Someone provides encrypted phones and SIM cards to operatives to coordinate attacks
- Cryptocurrency is converted and layered through exchanges to hide its destination before being transferred to a terrorist network

3.3 Bosnia and Herzegovina

BiH criminalises terrorist financing primarily through Article 202 of the state-level Criminal Code, a provision that MONEYVAL’s 2024 Mutual Evaluation Report describes as broad in scope and aligned with most requirements of the Terrorist Financing Convention. This article covers directly or indirectly giving, collecting or providing funds for a wide range of terrorism-related offences, including terrorism itself, public incitement, recruitment, training and several

³ International Convention for the Suppression of the Financing of Terrorism (1999) Art.1 para.1.

⁴ International Convention for the Suppression of the Financing of Terrorism (1999) Art.2.

⁵ Financial Action Task Force (2016).



aviation, maritime and nuclear safety offences. The law also extends to the financing of any conduct intended to intimidate the population or coerce domestic or international authorities, even where no attack is planned or executed. MONEYVAL emphasises that the offence explicitly criminalises financing a terrorist or a terrorist organisation for any purpose, which includes logistical, preparatory and travel-related support. Entity-level criminal codes contain similar provisions but are narrower, as only the state-level code covers all offences required under the Convention, which MONEYVAL notes is consistent with the distribution of competencies in BiH.

Across all four criminal codes, the TF offence applies to anyone who knowingly provides or collects funds that will be used, in whole or in part, by a terrorist organisation or an individual terrorist. According to MONEYVAL, this formulation is sufficiently broad to cover the financing of travel for terrorist purposes, a point also confirmed by the Ministry of Justice. The offence applies regardless of whether the funds come from legitimate or illegitimate sources, although MONEYVAL highlights inconsistencies in Republika Srpska where the definition of “property” does not fully reflect the FATF concept of “funds and other assets”. None of the criminal codes require the funds to be used for a terrorist act, nor must there be a link to a specific planned attack, a feature that MONEYVAL assesses as technically compliant with FATF standards. Intent or knowledge can be inferred from objective circumstances, which strengthens the practical usability of the offence, though MONEYVAL notes that this approach is not equally reflected in Brčko District legislation. Sanctions for TF range from one to ten years at the entity level and at least three years at the state level, and MONEYVAL considers them broadly proportionate and dissuasive. Liability of legal persons is formally established, but MONEYVAL identifies a structural limitation because liability applies only when the offence is committed in the interest of the legal person. Ancillary offences such as participation, attempt, aiding and abetting, association and facilitation are also covered in all jurisdictions. TF is a predicate offence for money laundering under the “all-crimes” approach, and the offence applies regardless of where the terrorist or terrorist organisation is located.

From an operational perspective, MONEYVAL’s 2024 findings make clear that the legal framework is broader than the way it is often applied in practice. Prosecutors and law enforcement officers do not need evidence of a planned attack before opening a TF investigation, because the law criminalises early forms of financial support, including travel preparation, logistical assistance and fundraising. Since intent can be established through objective financial behaviour, investigators should prioritise transaction patterns, networks and financial flows rather than waiting for explicit ideological indicators. The broad scope of the offence enables early intervention against facilitators, supporters and intermediaries, a point MONEYVAL highlights as under-utilised in current practice. MONEYVAL’s assessment also indicates that weaknesses in the liability of legal persons require investigators to focus on natural persons behind organisations and associations when indicators point to misuse. Overall, the legal framework gives prosecutors and LEAs wide room for action, but MONEYVAL stresses that its full potential depends on consistent interpretation, early use of financial intelligence and proactive engagement with the offence as a standalone crime.



4. Chapter Four - Patterns and red flags in Best Practices and Patterns in identifying terrorist financing

4.1 Introduction

This section describes how terrorist financiers exploit legitimate and illicit channels, it identifies emerging tools, outlines practical red flags, it emphasises the particular challenge of domestic terrorist financing where locally sourced, and it stresses the growing crime-terror nexus.

4.2 Typical methods of financing

Terrorists have been able to obtain funding from private financial benefactors.⁶ The FATF concluded that, 'wealthy private donors can be an important source of income for some terrorist groups'.⁷ Some of the most frequently used terrorist financing methods include the kidnapping for ransom,⁸ counterfeit currencies,⁹ oil refining,¹⁰ natural resources,¹¹ piracy,¹² Hawala,¹³ private donations and extortion.¹⁴ However, we have seen the emergence of new terrorism funding typologies. For example, 'low cost' terrorism has become a prominent typology as illustrated by the terrorist attacks in Madrid,¹⁵ London,¹⁶ London,¹⁷ Paris,¹⁸ London¹⁹ and Manchester.²⁰ Other emerging terrorist financing typologies include fraud.²¹ Here, terrorists have obtained funding via passport fraud, immigration fraud, identity fraud, financial fraud, online fraud, public funding and grant fraud, benefit fraud, student loan fraud, non-profit organisation fraud, tax fraud, counterfeiting, insurance fraud, mortgage fraud and trade-based fraud.²² Terrorists have been able to obtain funding from cryptocurrencies and social networking platforms.²³ The anonymity and speed provided by the internet is an appealing tool for terrorists to solicit financial donors. There is evidence that terrorist financiers have established relationships with organised criminal gangs (OCGs). This association has been described as the 'crime terror nexus'.²⁴ Here, terrorist financiers have

⁶ United States Department of Treasury (2015).

⁷ Financial Action Task Force (2015a), p. 13.

⁸ Ibid, p. 18.

⁹ Financial Action Task Force (2012).

¹⁰ Financial Action Task Force (2015a).

¹¹ Ibid, pp. 39-42.

¹² Financial Action Task Force (2011).

¹³ Financial Action Task Force (2013).

¹⁴ Financial Action Task Force (2015a).

¹⁵ Napoleoni (2007).

¹⁶ HM Government (2005), p. 23.

¹⁷ BBC News (2014).

¹⁸ CNN (2015).

¹⁹ BBC News (2017).

²⁰ Ryder et al (2023).

²¹ Ryder (2024).

²² Ibid.

²³ Wagman (2022).

²⁴ Basra and Neumann (2016).



exploited the OCGs infrastructure to raise funds via sexual and gender-based violence,²⁵ human trafficking²⁶ and drug trafficking.²⁷ Finally, the unprecedented scale of Islamic State of Iraq and Levante's (ISIL) finances illustrated 'corporate' or 'hierarchical' typology.²⁸ This can also be referred to as 'economy based' terrorist financing.²⁹

4.3 Indicators and 'red flags' in transactions and client behaviour

Transaction-based red flags of terrorist financing can include frequent small cash deposits or withdrawals structured to avoid reporting thresholds, known as smurfing.³⁰ Unusual international wire transfers, especially to or from high-risk jurisdictions or conflict zones, are also common indicators.³¹ Transactions that are inconsistent with a customer's known profile, such as large transfers from a student or unemployed individual, may raise concerns.³² The use of multiple accounts or intermediaries to obscure the origin or destination of funds, and frequent ATM activity across borders, particularly in areas linked to terrorism, are additional red flags.³³ Customer profile indicators focus on behaviour and documentation. These include a lack of clear business rationale for financial activity, reluctance to provide information or use of false identification, and sudden changes in account behaviour such as dormant accounts becoming active with large transactions. The use of personal accounts for business-like transactions, especially involving international transfers, is another warning sign. Organizational and sectoral red flags are particularly relevant for non-profit organizations (NPOs) and charities.³⁴ Financial activity that does not align with the stated purpose or geographic scope of an NPO, or large transfers to individuals or entities in high-risk areas without clear justification, may indicate misuse.³⁵ Shell companies or opaque ownership structures used to move funds across.³⁶

4.3.1 Detection indicators

Relevant for FIUs and financial institutions, are primarily transactional and behavioural red flags. These include patterns such as smurfing (structured small cash deposits), unusual international wire transfers, inconsistent customer profiles (large transfers by unemployed individuals), use of multiple accounts or intermediaries, and suspicious activity in dormant accounts. Red flags also extend to customer and organizational behaviours, such as reluctance to provide identification, use of personal accounts for business-like transactions, or non-profit

²⁵ Kenny and Malik (2019).

²⁶ Coonan and Thompson (2005).

²⁷ Williams (2007).

²⁸ Ryder (2018b).

²⁹ Brisard and Martinez (2014).

³⁰ Ryder (2020).

³¹ National Commission on Terrorist Attacks Upon the United States (2004).

³² Ryder *et al* (2023).

³³ Ryder (2024).

³⁴ Financial Action Task Force (2015b).

³⁵ Ibid.

³⁶ Baradaran *et al* (2013).



organizations conducting financial activity inconsistent with their stated mission or geographic scope.

4.3.2 Evidentiary indicators

These are used by law enforcement and prosecutors, are more substantive and contextual, often linked to specific criminal typologies and intent. These include the use of private donations, Hawala, fraud (identity, benefit, or tax fraud), cryptocurrencies, and exploitation of OCGs for funding through human trafficking or drug trade. These indicators help establish criminal intent, networks, and methods—critical for building legal cases and proving offences in court.

Therefore, the detection indicators serve as early warning signs to flag suspicious activity, while evidentiary indicators provide the legal and investigative foundation to prosecute terrorist financing offences.

4.4 Key Detection Indicators in BiH

4.4.1 Western Union Transfers and Informal Value Transfers:

Examples could include:

- Frequent small-value transfers via Western Union or other Money or Value Transfer Services (MVTs) from high-risk jurisdictions (e.g., Gulf countries, Turkey) to individuals or small businesses in BiH
- Structuring of remittances: Multiple senders from the diaspora sending funds to the same recipient or household, potentially masking the true origin or purpose of funds
- Lack of economic justification: Recipients with no declared income or business activity receiving frequent or large transfers
- Use of third-party senders: Transfers made by individuals with no familial or business ties to the recipient, raising questions about the legitimacy of the transaction

4.4.2 Diaspora Remittances

Examples could include:

- Over-reliance on remittances: BiH receives significant inflows from its diaspora, particularly from Western Europe and the Gulf. While most are legitimate, the volume and informality of channels (hand-carrying cash or using unregistered intermediaries) can create vulnerabilities
- Mismatch with declared income: Individuals receiving large remittances while reporting minimal or no income domestically
- Use of remittances to fund NPOs or religious institutions without clear oversight or transparency



4.4.3 Non-Profit Organizations (NPOs)

Examples could include:

- NPOs operating in conflict zones (Syria, Iraq) or sending funds to high-risk jurisdictions without clear humanitarian justification
- Lack of transparency in donor identity: donations from anonymous or foreign sources, especially from jurisdictions with weak AML/CFT controls (could reference list provided by EU, FATF and US)
- Unusual financial activity: NPOs with limited local presence but high-volume international transactions, or those using personal accounts for organizational funds
- Mission drift: NPOs conducting activities inconsistent with their stated objectives or geographic scope (e.g., a charity registered for education funding construction projects abroad)

4.4.4 Car Trade Sector

Examples could include:

- Cash-intensive transactions: car dealerships accepting large cash payments without proper documentation or customer due diligence
- Use of front businesses: import-export companies dealing in used vehicles as a cover for moving funds across borders
- Rapid turnover of high-value vehicles: frequent buying and selling of cars without clear commercial rationale, potentially used to layer illicit funds
- Cross-border anomalies: Vehicles imported from or exported to jurisdictions with known terrorist financing risks, often involving under-invoicing or false documentation

4.4.5 Construction Materials and Real Estate

Examples could include:

- Over-invoicing of materials: Inflated invoices for cement, steel, or other materials used to justify large fund transfers
- Use of shell companies: Entities with no physical presence or staff involved in construction supply chains
- Unusual project financing: Construction projects funded by foreign donors or NPOs with opaque financial trails
- Cash-based purchases: Real estate or materials bought in cash, especially in areas with known radicalization risks or limited regulatory oversight

4.5 Domestic Terrorist Financing Threats

Domestic terrorist financing poses a significant and evolving threat, enabling groups and individuals to sustain operations and exploit financial systems with increasing sophistication.



Domestic terrorist financing refers to the funding of terrorist activities that originate and operate within a country's borders, often driven by ideologies such as far-right extremism, religious fundamentalism, or anti-government sentiment.³⁷ Unlike international terrorism, domestic actors typically rely on small-scale, low-cost operations, making detection more difficult. They often use legal sources of income such as employment, donations, the sales of merchandise, crowd funding, private donations, cryptoassets, membership fees, online content, paraphernalia and Merchandise, events/mass gatherings, subscriptions and inheritance.³⁸ There are increasingly intertwined with broader criminal activity, including fraud and illicit trade.³⁹ A key concern is the use of virtual assets and online platforms to raise and move funds. Terrorist actors exploit crowdfunding sites, social media, and encrypted messaging apps to solicit donations and coordinate financial flows.⁴⁰ The FATF's 2025 update warns that domestic groups are leveraging these technologies to bypass traditional financial controls, often operating in fragmented cells that are harder to monitor FATF.⁴¹

Key investigative takeaways:

- Small, frequent, low-value transactions are a common funding pattern and can indicate sustained operational support despite low individual amounts
- Blending of legitimate and illicit income (employment, sales, donations, subscriptions, inheritance) is used to obscure purpose and provenance
- Use of online platforms and virtual assets greatly expands reach and complicates traceability
- Fragmented cell structure and decentralized networks reduce single-point visibility and shift activity to peer-to-peer channels
- Convergence with other crimes (fraud, illicit trade) creates parallel revenue streams and transactional complexity that conceal terrorist financing
- Public-facing fundraising tied to ideological messaging (merchandise, content monetization, event receipts) provides plausible deniability while funding operations

Financing typologies (common models):

- Microdonations / Crowdfunding: many small donations via platforms, social media appeals, or encrypted requests
- Merchandise and content monetization: sales of paraphernalia, subscriptions, paid content, and membership fees channel income under commercial cover
- Peer-to-peer and informal transfers: cash handoffs, person-to-person electronic payments, gift cards, or informal networks to move funds off-radar
- Crypto and virtual assets: direct crypto donations, mixers, stablecoins, NFT sales, or peer-to-peer transfers to obfuscate origin and destination

³⁷ Financial Action Task Force (2021).

³⁸ Ibid.

³⁹ UK Government (2025).

⁴⁰ Ryder (2020).

⁴¹ Financial Action Task Force (2025c).



- Criminal enterprise proceeds: fraud, smuggling, theft, or illicit trade routed into organizational coffers
- Events and mass gatherings: ticket sales, onsite donations, and ancillary merchandise used to collect funds and recruit
- Private/network donations and inheritance: targeted wealthy supporters, family transfers, or legacy funds acting as clean source of capital

Practical red flags for investigators

Financial behaviour:

- Multiple small deposits or withdrawals that aggregate to operationally meaningful amounts
- Sudden increase in payment activity tied to ideological events, online campaigns, or spikes in content engagement
- Transactions inconsistent with stated occupation/income or lifestyle mismatches
- Frequent transfers to many small recipients or rapid, repeated transfers through different accounts

Channels and tools

- Use of crowdfunding and donation platforms with vague or coded appeals (no clear charitable purpose)
- Payments routed through crypto wallets, mixers, or privacy coins without corresponding legitimate business activity
- Use of pre-paid cards, gift cards, or reloadable instruments to move value anonymously
- Dependence on encrypted messaging apps for fundraising instructions or payment coordination

Organizational and operational markers

- Merchandise sales or events where proceeds are not reconciled or routed through opaque entities
- Multiple small businesses or online storefronts with limited commercial activity but steady inflows
- Intermingling of legitimate membership fees/subscription income with direct operational expenses
- Networked donations from geographically dispersed supporters without clear family/charitable ties

Communications and public signals

- Public ideological recruitment combined with fundraising asks framed as 'support', 'defence', or 'legal defence' of members.
- Use of coded language, hashtags, or burner accounts to solicit funds.



- Rapid account turnover or use of ephemeral platforms to avoid traceability

Suggested investigative priorities

- Monitor aggregation patterns: focus on clusters of small transactions, timing correlations with online campaigns or events
- Trace platform linkages: map donor flows from crowdfunding, social media links, and payment processors to downstream accounts or crypto wallets
- Follow the merchandise and event money trail: require receipts, vendor contracts, and bank reconciliation for suspected outlets
- Use financial-communications correlation: pair transactional data with open-source monitoring of messaging channels to link appeals to receipts
- Target convergence with crime: investigate suspicious businesses or individuals for dual criminal-financial activities (fraud, smuggling)
- Leverage multi-disciplinary evidence: combine financial, digital-forensic, and human intelligence to overcome decentralized and encrypted operations

Eastern European countries face a diverse range of domestic terrorist threats. According to Europol, several Eastern EU Member States reported completed or foiled attacks linked to ideologically motivated domestic actors Europol.⁴² These groups often operate in fragmented cells, using legal income streams and small-scale criminal activities to fund operations. The Royal United Services Institute (RUSI) highlights the growing relevance of the crime-terror nexus in Eastern Europe, where terrorist actors exploit organized criminal networks for logistical and financial support.⁴³ BiH faces a persistent but under-resourced threat from domestic terrorist financing, shaped by its post-conflict legacy, political fragmentation, and exposure to radicalization networks. While the scale of domestic terrorism is limited, vulnerabilities in financial oversight and institutional coordination create significant risks. Bosnia's domestic terrorist financing landscape is influenced by residual extremist ideologies from the 1990s conflict, including ethno-nationalist and religiously motivated actors. According to the U.S. State Department, Bosnia remains a cooperative counterterrorism partner but struggles with limited institutional capacity and fragmented governance structures.⁴⁴ A key concern is the return of foreign terrorist fighters (FTFs) and their families from Syria and Iraq.⁴⁵ Bosnia outlawed foreign fighting in 2014 and has repatriated several nationals, but reintegration and monitoring remain weak points.⁴⁶ These returnees may pose financing risks through informal networks, unregulated donations, or exploitation of non-profit organizations.

⁴² Europol (2025).

⁴³ Royal United Services Institute (2025).

⁴⁴ United States Department of State, Country Reports on Terrorism 2023: BiH (Bureau of Counterterrorism, 2023).

⁴⁵ Counter Extremism Project (n/d).

⁴⁶ United States Department of State (2023).



Investigative takeaways:

- Fragmented cell structures decrease centralized visibility and require correlation across small, dispersed actors
- Crime–terror nexus: collaboration with organized criminal networks provides logistics and covert financing channels
- Legal cover for funding: use of lawful income streams and small-scale crime obscures origin and intent
- Institutional and oversight gaps create exploitable vulnerabilities where weak governance and limited capacity allow flows to go undetected
- Returnee risk multiplier: returning foreign fighters and their networks can introduce new funding sources and informal channels
- Historical and ideological drivers influence long-term fundraising patterns tied to ethno-nationalist and religious narratives

Common regional typologies:

- Organized-criminal-enabled financing: proceeds from smuggling, trafficking, or organized crime laundered into extremist activity
- Low-value, distributed funding: many small donations and micro-revenue sources (sales, events, membership fees) aggregated to support operations
- Informal network transfers: cash couriers, remittances, friendship/family transfers, or unregulated money agents moving value across borders
- Exploitative non-profit misuse: charities, NGOs, or community groups used as fronts for collecting and distributing funds
- Post-conflict legacy funding: resources and sympathies remaining from past conflicts redirected toward modern extremist activity

Practical red flags for investigators:

- Discrepancy red flags: incomes or business activity inconsistent with transactional volume or sudden unexplained inflows
- Unaccounted aggregation: multiple small deposits across accounts or entities that cumulatively fund operations
- Links to organized crime: transactional or social-network connections to known criminal groups or suspicious commercial fronts
- Opaque beneficiary patterns: funds routed through shell entities, informal intermediaries, or repeated use of cash couriers
- Non-profit anomalies: charities or local organizations with poor bookkeeping, rapid donor increases, or unexplained transfers abroad
- Returnee-associated channels: donations, remittances, or support appearing soon after repatriation or tied to known returnee networks
- Cross-border microflows: repeated small cross-border transfers lacking legitimate commercial rationale



Investigation priorities and tactics:

- Network mapping: link financial records to open-source indicators of ideology, membership, and criminal associations
- Follow-the-money across modalities: combine bank, cash, crypto, and informal transfer traces to see aggregation points
- Scrutinize non-profits and events: obtain vendor contracts, bank reconciliations, and donor lists for organizations in the ideological ecosystem
- Target organized-crime connections: prioritize probes where financial flows intersect with known illicit trade routes or actors
- Monitor returnee influence: track financial activity around repatriation timelines and associated contacts
- Enhance interagency coordination: address governance fragmentation by sharing financial intelligence between law enforcement, financial supervisors, and counterterrorism units

4.6 Crime-Terror Nexus

The crime-terror nexus refers to the collaboration between criminal and terrorist groups, often resulting in hybrid organizations that blur the lines between political violence and profit-driven crime. The nexus describes the intertwined relationship between organized crime and terrorism. Traditionally viewed as distinct phenomena, one is motivated by profit, the other by ideology, yet these groups have found common ground in operational needs, financial strategies, and territorial control.⁴⁷ The nexus can manifest in several forms including collaboration between separate criminal and terrorist entities.⁴⁸ One common pathway is terrorist conversion, where ideologically driven groups adopt criminal activities such as drug trafficking,⁴⁹ extortion,⁵⁰ or smuggling to fund their operations.⁵¹ This shift allows them to sustain themselves financially while pursuing political goals. Conversely, some criminal organizations may adopt terrorist tactics to protect their interests or exert influence, though this is less common. The relationship is also shaped by shared use of technologies, illicit markets, and logistical networks.⁵² Online platforms, encrypted communications, and global financial systems have lowered barriers to cooperation, enabling rapid knowledge transfer and cross-border operations.⁵³

⁴⁷ Basra and Neumann (2016).

⁴⁸ Ryder (2025).

⁴⁹ Williams (2007).

⁵⁰ Financial Action Task Force (2015).

⁵¹ Sinaee and Khatibi (2023).

⁵² Ryder (2025).

⁵³ Ibid.



5. Chapter Five - Circumstances that may indicate terrorist financing

Certain financial activity such as smurfing, the use of humanitarian fronts, and unconventional asset transfers can serve as red flags for terrorist financing, especially when combined or lacking legitimate economic rationale.⁵⁴ Terrorist financing often involves smurfing, a technique where large sums are broken into smaller, less suspicious transactions to avoid detection thresholds.⁵⁵ These deposits may be made across multiple bank branches or accounts, often by individuals with no clear connection to the funds. The aim is to obscure the origin and destination of money, making it harder for financial institutions and authorities to trace the flow.⁵⁶

Another common tactic is the exploitation of humanitarian causes.⁵⁷ Terrorist groups may establish or infiltrate charities and NGOs to raise funds under the guise of disaster relief, education, or medical aid.⁵⁸ These entities can serve as both fundraising platforms and logistical support hubs.

Cash transfers and Hawala networks remain prevalent in terrorist financing due to their anonymity and limited documentation.⁵⁹ Cash couriers can physically move funds across borders, bypassing formal financial systems.⁶⁰ Hawala, an informal value transfer system based on trust and family networks, is especially vulnerable to abuse because it operates outside conventional banking channels and often lacks a paper trail.⁶¹

Terrorist financiers may also invest in property, luxury goods, and virtual assets to store or move value discreetly.⁶² Real estate transactions, especially those involving undervalued or overvalued properties can be used to hide illicit funds. Similarly, high-value items like watches, art, or vehicles can be used to launder money or facilitate trade-based terrorist financing. The rise of virtual assets such as cryptocurrencies has added complexity, enabling cross-border transfers with limited regulatory oversight and pseudonymous accounts.⁶³

5.1 Typical Methods of Terrorist Financing in BiH

Terrorist financing in BiH commonly relies on small-value cash contributions collected within family, social and religious networks. These funds are usually raised informally during gatherings where no structured financial oversight exists. Support networks linked to

⁵⁴ Gordon (2011).

⁵⁵ Irwin et al (2011).

⁵⁶ Ryder (2015).

⁵⁷ Crimm (2003).

⁵⁸ Bauer and Levitt (2020).

⁵⁹ Freeman and Rueshen (2011).

⁶⁰ Ibid.

⁶¹ Van de Bunt (2008).

⁶² Cheney (2005).

⁶³ Ryder (2020).



individuals who travelled to Syria or Iraq often depend on personal cash transfers that remain below reporting thresholds and are typically presented as ordinary family assistance.

Misuse of humanitarian initiatives is one of the most persistent domestic risks. Informal charity drives are sometimes organised without registration or documentation, allowing part of the collected funds to be diverted to individuals associated with extremist environments. Registered non-profit organisations also remain vulnerable when operating with limited financial controls, parallel accounts or substantial cash-based activity.

This includes organisations presenting themselves as religious, cultural or humanitarian while lacking transparent governance procedures.

Cross-border cash movement remains a realistic method of transferring funds. The combination of a long land border, difficult terrain and numerous informal crossing points allows individuals to move small amounts of undeclared cash with limited detection. Informal value-transfer arrangements, including hawala-type systems, also play a significant role. These mechanisms rely on trusted intermediaries within local communities or migrant networks and enable rapid, undocumented cross-border movement of funds outside the regulated financial system. Their reliance on personal trust and the absence of any financial footprint make them particularly attractive for returnees, sympathisers and facilitators.

Online fundraising and social media campaigns are increasingly used to collect money, often presented as humanitarian assistance. These campaigns typically involve small, frequent payments that provide limited transparency regarding the ultimate recipient. Remittances from the Bosnian diaspora represent a further channel that can be misused, especially when the stated purpose is vague or unverifiable. In some cases, TF-related funds are deliberately combined with legitimate family support to avoid scrutiny.

Cash-intensive businesses remain vulnerable to exploitation, particularly those with limited internal controls or high levels of unrecorded transactions. Unregistered money-exchange services present an additional risk due to uncontrolled cash inflows and the absence of reporting obligations. Individuals involved in low-level criminality may redirect part of their illicit proceeds to extremist associates, creating an overlap between petty criminal activity and the financing of terrorism.

Sale of personal property, including vehicles and electronics, is often used as a quick method of generating funds for travel or logistical support. Community fundraising intended for conflict-affected populations has also been misused by diverting a portion of the donations. Money transfer services such as Western Union remain susceptible to low-value, high-frequency transfers with minimal narrative information.

The non-profit sector overall continues to face elevated exposure to TF risks. Organisations relying heavily on cash donations, maintaining weak governance structures or receiving foreign funding from unverifiable sources are particularly vulnerable. Funds collected during religious lectures or informal community gatherings are at heightened risk when financial reporting is absent. Individuals with access to bank accounts in multiple jurisdictions can



move funds through small transfers to and from BiH to avoid triggering monitoring mechanisms.

Private loans between individuals represent an additional informal mechanism for moving TF-related funds without entering the regulated sector. Although still limited, the use of cryptocurrencies is slowly increasing, particularly among younger individuals experimenting with peer-to-peer wallets. Several investigations have identified attempts to convert cash into digital assets as a way to avoid financial monitoring.

Overall, terrorist financing in BiH tends to depend on personal trust networks, small-value transactions and informal movements of money. These features reduce visibility in the formal financial system and underscore the need for proactive financial intelligence, early investigative action and close coordination between prosecutors and law enforcement agencies.

5.2 Red Flag Indicators for Law Enforcement and Prosecutors in BiH

5.2.1 Cash and Low-Value Transactions

- Frequent small cash deposits or withdrawals inconsistent with the individual's income
- Informal cash collections during religious or social gatherings
- Individuals with limited legitimate income but regular access to significant cash

5.2.2 Hawala and Informal Value-Transfer Systems

- Transfers with no corresponding banking activity
- Funds received from multiple foreign locations in rounded, repetitive amounts
- Links to migrant groups or unregistered community intermediaries involved in moving money

5.2.3 Non-Profit Organisations:

- NPOs operating primarily in cash with limited documentation
- Fundraising activities without a clear list of beneficiaries
- NPOs managed by individuals associated with radical networks
- Foreign donations from sources that cannot be verified

5.2.4 Returnees and Support Networks:

- Cash transfers or donations directed to individuals who previously travelled to Syria or Iraq
- Fundraising for 'families in conflict zones' without transparency
- Increase in financial activity immediately following a person's return from a conflict area

5.2.5 Cash-Intensive Businesses and Unlicensed Exchange Services:

- Cash-heavy businesses reporting unusually low or inconsistent profits
- Use of unlicensed money-exchange operators



- Frequent currency exchanges without a credible economic purpose

5.2.6 Remittances and Cross-Border Transfers:

- Numerous small international transfers from high-risk jurisdictions
- Vague or generic payment descriptions such as 'help' or 'support'
- Use of multiple remittance providers within a short period

5.2.7 Cryptocurrency Activity:

- Purchase of cryptocurrency with cash
- Peer-to-peer crypto transfers without a clear source of funds
- Sudden crypto wallet activity among individuals known to frequent radical circles

5.2.8 Travel and Logistics:

- Payments for travel inconsistent with the individual's financial profile
- Combination of donations and sale of personal assets shortly before travel
- Transfers related to destinations associated with conflict or extremist activity

5.2.9 Behavioural Indicators:

- Reluctance to use banks or insistence on cash transactions
- Sudden shift in communication patterns, including use of intermediaries
- Increased association with radical lectures, groups or events vulnerable to extremist influence

Operational Table: TF Methods, Indicators and Investigative Actions in BiH

1. Cash and Low-Value Transactions

Method	Red Flag Indicator	Recommended Investigative Action
Small-value cash collections within communities	Frequent small deposits/withdrawals inconsistent with income	Obtain bank statements, compare with declared income, interview employer, analyse lifestyle vs income
Informal religious/social donations	Cash collected during gatherings with no records	Identify organisers, request NPO registration status, examine donor lists, conduct financial profiling
Cash-rich individuals with no stable income	Unexplained access to significant cash	Check criminal records, verify property ownership, cross-check with tax authorities

2. Hawala and Informal Value Transfers



Method	Red Flag Indicator	Recommended Investigative Action
Hawala-type transfers	Incoming/outgoing transfers with no banking footprint	Use financial intelligence from FIU, map personal networks, check travel history of intermediaries
Community brokers and migrant networks	Repetitive rounded foreign transfers	Conduct surveillance on suspected brokers, identify meeting points, obtain communications warrants
Informal intermediaries	Persons “helping send money” with no licence	Interview intermediaries, check criminal and immigration background, monitor cash deposits into their accounts

3. Non-Profit Organisation Abuse

Method	Red Flag Indicator	Recommended Investigative Action
Misuse of NPOs for TF	NPO with exclusively cash-based operations	Request full financial reports, examine cash books, verify donor lists, inspect premises
Parallel accounting	Missing or duplicate records	Seize accounting documents, compare declared and undeclared activities, interview treasurers
High-risk NPO leadership	Leaders with radical or foreign links	Conduct background checks, analyse travel records, review open-source content (lectures, sermons, posts)

4. Returnee Networks and Support Groups

Method	Red Flag Indicator	Recommended Investigative Action
Support to foreign fighter returnees	Transfers to returnees or their families	Cross-reference with intelligence files, interview family members, track spending pattern of returnees
Humanitarian fundraising for conflict zones	No transparent beneficiary lists	Verify recipients, request proof of distribution, analyse organiser’s digital communications



Financial activity increase after return	Sudden rise in transactions	Review travel documents, trace money trail, check communication with foreign persons
--	-----------------------------	--

5. Cash-Intensive Businesses and Unlicensed Exchange Services

Method	Red Flag Indicator	Recommended Investigative Action
Cash-only small businesses used as cover	High cash flow but low declared profit	Examine tax filings, conduct undercover visits, inspect invoices and suppliers
Unlicensed money exchange	Frequent large currency exchanges	Coordinate with market inspectors, seize cash and ledgers, monitor suspicious locations
Mixing business funds with TF	Inconsistent cash patterns	Review CCTV, analyse employee statements, track suppliers and customers

6. Remittances and Cross-Border Transfers

Method	Red Flag Indicator	Recommended Investigative Action
Misuse of diaspora remittances	Multiple small foreign transfers	Contact remittance providers, analyse senders' profiles, check connectivity between senders
Vague payment descriptions	"Help", "Support", "Donation"	Interview recipients, request FIU analysis with STR/CTR records, trace subsequent withdrawals
Multiple remittance channels used	Several providers in short period	Identify pattern, request internal logs of transfer providers, monitor recipient's cash-out activity

7. Cryptocurrency

Method	Red Flag Indicator	Recommended Investigative Action
Use of crypto to hide TF	Cash converted into crypto	Request VASP records, seize devices, analyse transaction hashes via blockchain tools
Peer-to-peer crypto transfers	No clear source of funds	Investigate communication channels, inspect wallet



		activity, link wallets to known entities
New crypto activity among radical circles	Sudden use of apps or exchanges	Monitor devices, analyse chat groups, track fiat-to-crypto conversion points

8. Travel and Logistics Funding

Method	Red Flag Indicator	Recommended Investigative Action
Travel to high-risk countries	Ticket purchases inconsistent with income	Obtain travel manifests, analyse financial capability, inspect luggage and digital devices
Sale of personal assets before travel	Quick liquidation of goods	Identify buyers, track proceeds, verify purpose of travel
Mixed donations and self-funding	Several contributors for one person's travel	Investigate donor profiles, map the network, check ideological links among contributors

9. Behavioural Indicators

Method	Red Flag Indicator	Recommended Investigative Action
Avoidance of banks	Insistence on cash only	Interview subject, collect open-source intelligence, perform lifestyle analysis
Sudden shift in communications	Use of intermediaries or encrypted apps	Apply digital forensics, analyse communication patterns, cross-reference contacts
Radicalisation signals	Attendance at risky lectures or groups	Coordinate with intelligence agencies, run social-media profiling, document extremist narratives

5.3 BiH Typologies

In BiH, several typologies of terrorist financing reflect the country's unique vulnerabilities, particularly the misuse of small NGOs, informal remittance channels, and cash-based transactions. These methods often lack a clear economic rationale and are frequently structured to evade detection thresholds.

5.3.1 Structured Cash Deposits (Smurfing):



Terrorist financing networks have employed smurfing to fragment large sums into smaller deposits below reporting thresholds. These are often conducted across multiple bank branches or money transfer outlets (e.g., Western Union), sometimes by individuals with no familial or economic link to the originator.

- Red flags: Frequent small cash deposits by unrelated individuals; use of multiple remittance agents in different municipalities
- Evidence sources: STRs from banks and money transfer operators; CCTV footage; teller logs; account holder interviews
- Investigative actions: Transaction pattern analysis; tracing linked accounts; cross-referencing with travel and communication records

5.3.2 Misuse of Small NGOs and Humanitarian Fronts:

Small, under-regulated NGOs could be exploited to raise and channel funds under the guise of charitable or religious activities. Some have received foreign donations earmarked for humanitarian aid but diverted to support terrorist actors domestically or abroad.

- Red flags: Disproportionate foreign donations; vague project descriptions; cash withdrawals shortly after receipt of funds.
- Evidence sources: NGO registration and financial disclosures; donor correspondence; customs declarations; field inspections.
- Investigative actions: Auditing NGO financials; verifying project implementation; interviewing staff and beneficiaries; tracing donor flows.

5.3.3 Remittance Systems and Informal Transfers:

Remittance services like Western Union are used for terrorist financing due to their speed, accessibility, and limited customer due diligence. Funds are often sent from diaspora communities or conflict zones with minimal documentation.

- Red flags: High-frequency inbound transfers from high-risk jurisdictions; use of aliases or third-party pickups; inconsistent declared purposes.
- Evidence sources: MTO transaction logs; sender/receiver ID records; phone metadata; border crossing data.
- Investigative actions: Mapping remittance flows; interviewing recipients; liaising with foreign FIUs; deploying undercover test transactions.

5.3.4 Cash Couriers and Cross-Border Transfers:

Physical cash smuggling is a viable terrorist financing method. Funds may be concealed in vehicles or personal belongings and moved to neighbouring jurisdictions.

- Red flags: Frequent cross-border travel without economic justification; undeclared currency; inconsistent travel narratives.
- Evidence sources: Customs seizure reports; vehicle searches; travel manifests; canine unit alerts.
- Investigative actions: Surveillance at border crossings; joint operations with neighbouring countries; forensic examination of seized cash.



5.3.5 Real Estate and High-Value Goods:

Terrorist financiers may invest in real estate or luxury goods to store value or launder proceeds. Undervalued property purchases and unexplained wealth accumulation are common indicators.

- Red flags: Purchases by individuals with no declared income; use of cash or third-party intermediaries; rapid resale at inflated prices.
- Evidence sources: Land registry data; notarial records; tax filings; lifestyle audits.
- Investigative actions: Asset tracing; beneficial ownership checks; valuation comparisons; interviews with real estate agents.

5.3.6 Virtual Assets and Online Fundraising:

While still emerging, cryptocurrencies and online crowdfunding platforms are increasingly used to solicit and transfer terrorist financing related funds.

- Red flags: Use of privacy coins; donations to anonymous wallets; social media fundraising with ideological messaging
- Evidence sources: Blockchain analytics; platform takedown reports; open-source intelligence (OSINT)
- Investigative actions: Wallet tracing; coordination with VASPs; monitoring extremist online ecosystems.

5.4 Financial investigations

Financial investigations are structured inquiries into the financial behaviour, assets, transactions, and economic relationships of individuals or organisations suspected of involvement in criminal activity. Their purpose is to explain where money comes from, how it moves, who controls it, and how it supports criminal conduct. Financial investigations reveal hidden networks, facilitators, intermediaries, and assets that can be frozen or confiscated. Because financial data is objective and less prone to manipulation than statements or human intelligence, it provides a reliable evidentiary foundation. It also generates early indicators in terrorism related cases, where financial behaviour often precedes operational activity. The text that follows is based on the FATF Operational Issues – Financial Investigations Guidance.⁶⁴

According to the FATF Guidance on Operational Issues and Financial Investigations, financial investigations are a standard component of all serious and cross border crime inquiries. They help identify unexplained wealth, beneficial ownership, and suspicious financial patterns, and they improve coordination among FIUs, tax authorities, border control, customs, banks, prosecutors, and law enforcement agencies. By uncovering networks rather than individuals, they transform isolated information into a coherent picture of criminal organisation and support both criminal cases and the implementation of targeted financial sanctions under relevant United Nations Security Council resolutions.

⁶⁴ FATF Operational Issues – Financial Investigations Guidance (2012).



Financial investigations in money laundering cases differ from those in terrorist financing cases. Money laundering focuses on “dirty money” derived from a predicate offence and often seeks to hide its criminal origin. Terrorist financing frequently involves “clean money” from legitimate sources that is used for an illicit purpose. Terrorist financing investigations therefore emphasise purpose, destination, and behavioural indicators rather than the source of funds. Low value, repetitive, or behaviourally unusual transactions can carry far more significance in terrorist financing cases than in money laundering cases, especially when linked to travel, recruitment, logistics, or support to designated organisations or individuals.

Financial behaviour often provides the earliest detectable signals of travel facilitation, recruitment, logistics, propaganda support, or safe house management. Unlike money laundering, where the financial investigation often follows the predicate offence, financial investigation in terrorist financing should guide and shape the broader counter terrorism picture from the beginning. It supports prosecution, prevention, intelligence assessment, and the application and review of targeted financial sanctions.

For BiH, financial investigations offer a cost-effective method for detecting networks that are otherwise difficult to identify. When properly integrated, financial investigations enhance early detection, strengthen operational coordination, and improve asset recovery.

Financial investigation is the most reliable method for uncovering entire networks rather than isolated offenders. It provides earlier, stronger, and more durable evidence than traditional investigative tools. Without it, terrorist financing cases remain fragmented and much harder to prove, and the system struggles to show real effectiveness against the threats identified in national and supranational risk assessments.

5.5 Core FATF Operational Principles Relevant to TF Investigations

This section outlines the core FATF operational principles that underpin effective financial investigations in terrorist financing cases. These principles form the global benchmark for investigative practice and reflect what evaluators expect to see in real cases. Applying them consistently strengthens early detection, improves coordination, supports successful prosecutions, and demonstrates effectiveness under Immediate Outcome 6 and Immediate Outcome 10.

Early Financial Investigation as Standard Procedure

According to FATF Guidance, every terrorism case should immediately trigger a financial investigation. The financial component must start at the same time as any operational or intelligence led inquiry. Investigators should not wait for a visible financial “problem” before examining accounts, transfers, and assets. This is essential because terrorist financing activity often appears through micro transactions, informal transfers, donations, or behavioural anomalies that disappear quickly if not addressed. Early review of available reports from obliged entities, including suspicious transaction reports with terrorist financing indicators, should be part of this automatic response.



Why this matters?

Early financial investigation prevents the loss of key financial evidence. It increases the likelihood of discovering networks rather than isolated offenders and aligns practice with FATF expectations on effectiveness. It also allows authorities to detect and act on preparatory behaviour before it escalates into an operational threat.

Parallel Investigations

Parallel investigations mean that authorities investigate the terrorism related offence and the terrorist financing offence at the same time. Financial investigators work in close coordination with case officers dealing with operational, intelligence, or public order aspects. Information and evidence flow in both directions, so that financial findings support the terrorism case and operational findings support the financial case.

Parallel investigations reveal facilitators, supporters, logisticians, and enablers who may not be visible through traditional policing. They also expose how money is raised, stored, moved, and spent in support of terrorist purposes, including how funds relate to travel, safe houses, propaganda, weapons, or support to individuals associated with terrorist organisations.

Why this matters?

Parallel investigations create a complete operational and financial picture. They strengthen evidentiary logic, help establish intent and knowledge, and allow prosecutors to address both terrorist acts and their financing in a coherent way. This integrated approach is critical for securing convictions and effective confiscation orders.

Multi-Disciplinary Task Forces

FATF promotes multi-disciplinary task forces that bring together financial investigators, FIU analysts, prosecutors, cyber experts, border police, customs officers, tax authorities, and bank liaison officers. In BiH, where competencies are fragmented across several institutions and levels of government, this model is particularly important.

A typical task force for terrorist financing cases could include:

- specialised financial investigators from the central investigative service;
- a prosecutor responsible for terrorism and terrorist financing;
- an FIU analyst with access to STRs, CTRs, and other financial reports;
- an intelligence service liaison for national security input;
- customs and border officials for cash and cross border movement data;
- IT and digital forensics experts, including virtual asset specialists; and
- a liaison officer from the banking or payment services sector where appropriate.

The task force should have clear leadership, defined roles, agreed information sharing procedures, and regular joint case meetings. It should also have the capacity to prioritise high risk cases identified through STRs, national risk assessments, and security intelligence.



Why this matters?

No single institution has the full picture in terrorist financing cases. Multi-disciplinary task forces reduce information gaps, avoid duplication of effort, and improve the speed and quality of operational decision making. They also help ensure that information relevant for targeted financial sanctions or designation proposals is not lost within a single institution.

Asset Tracing and Confiscation as a Core Objective

Asset tracing and confiscation must be planned from the beginning of every terrorist financing case. Investigators should not wait for a conviction before thinking about assets. Even assets of modest value can have high operational significance if they fund travel, safe houses, weapons, propaganda, or recruitment.

Authorities should consider all options for asset recovery, including criminal confiscation, non-conviction-based confiscation where available, and administrative measures where appropriate. In terrorist financing cases, asset freezing measures related to targeted financial sanctions regimes can complement criminal confiscation but do not replace the need to pursue judicial asset recovery. Asset management units should be able to safeguard and, when necessary, dispose of frozen or seized property.

Why this matters?

Confiscation disrupts terrorist financing networks by removing the resources they need to operate. It provides a concrete, measurable outcome that demonstrates effectiveness, which is central to FATF assessments under Immediate Outcome 6 and 10. It also sends a strong deterrent message to facilitators and supporters.

Access to Registries and Beneficial Ownership Information

Investigators must have rapid and reliable access to:

- company and commercial registries;
- registers of non-profit organisations;
- land and real estate registries;
- vehicle registration systems;
- telecom subscriber records; and
- border crossing and passenger data.

These sources are essential for identifying beneficial owners, front companies, informal structures, and the real controllers of assets and accounts. Where possible, registries should be electronic, searchable, and updated in real time. Access procedures should be clearly regulated and operational staff trained to interpret the information correctly, including in cases where nominees or complex structures are used.

Why this matters?

Beneficial ownership information allows investigators to see through front structures and nominees. Without it, key facilitators remain hidden behind legal entities or informal arrangements, and investigations become slower and less effective. Reliable registries are also



necessary to support asset freezing and confiscation and to provide credible information to international partners.

5.6 Minimum Operational Expectations for LEAs and Prosecutors

This section sets out the minimum actions that law enforcement agencies and prosecutors should take in every terrorist financing case. Standardising these steps reduces the risk of omissions, improves consistency, and ensures that essential evidence is preserved and exploited. These expectations should complement, not replace, agency specific procedures, and should be embedded in internal guidance, training, and supervision.

Immediate Actions in Any TF Case

Investigators should, as a minimum:

- Launch a parallel financial investigation from day one;
- Request FIU analytical products, including STR and CTR analysis and network charts, and review whether STRs with TF indicators have already been filed;
- Identify all bank accounts, payment cards, remittance channels, and MVTs activity linked to the subject and key associates;
- Conduct a rapid asset and lifestyle assessment, comparing declared income with observed expenditure and assets;
- Map cross border transfers, including flows from and to high-risk jurisdictions and diaspora communities;
- Check for links to non-profit organisations, informal fundraising groups, and charity structures, including any previous supervisory findings or compliance issues;
- Analyse travel and border crossing data, and correlate movements with financial activity and communication patterns;
- Examine virtual asset and digital wallet activity where relevant, including possible use of peer-to-peer platforms and unlicensed providers;
- Identify potential facilitators, intermediaries, and supporters in the financial chain, not only those directly engaged in operational activities; and
- Prepare early, well-grounded recommendations for the freezing or restraint of assets under both criminal law and, where appropriate, targeted financial sanctions mechanisms.

Why this matters?

The first days of an investigation are critical. Rapid, structured action prevents the loss of financial evidence, sets a clear investigative direction, and increases the chances of identifying the full network rather than only the main suspect. It also shows that the jurisdiction can respond promptly to high-risk signals from obliged entities and intelligence services.

Expectations for Prosecutors

Prosecutors handling terrorist financing cases should:

- Guide investigators to focus on financial behaviour from the outset;
- Issue timely and well targeted orders for bank records, telecommunications data, and digital forensics;



- Work closely with the FIU to understand and use financial intelligence, including clarifying analytical questions in direct meetings;
- Develop an early strategy for freezing and confiscating assets, including consideration of non-conviction-based tools where available;
- Ensure that facilitators, intermediaries, and supporting entities are included in the case theory where justified, rather than focusing only on the main subject; and
- Monitor the progress of both operational and financial investigations to ensure that they remain coherent and mutually reinforcing.

Why this matters?

Prosecutors set the legal direction and tempo of the case. Early, proactive engagement by the prosecutor improves evidentiary quality, strengthens legal reasoning, and increases the likelihood of a successful conviction and confiscation. It also helps align criminal proceedings with the application of targeted financial sanctions where appropriate.

5.7 Financial Intelligence Exploitation and FIU–LEA Cooperation

The financial intelligence unit is a central provider of data and analysis for terrorist financing investigations. Effective cooperation between the FIU and law enforcement determines how quickly and how deeply financial information can be exploited. This cooperation should be structured, predictable, and based on clear roles and expectations, rather than ad hoc exchanges.

Central Role of the FIU in TF Investigations

The FIU should be fully integrated into the terrorist financing investigative process. It should be able to provide:

- Analysis based on suspicious transaction reports and currency transaction reports;
- Historical and current account information from reporting entities;
- Network diagrams showing relationships between subjects, accounts, and entities;
- Information on cross border cash declarations and seizures;
- Analysis of diaspora remittances and money value transfer services; and
- Intelligence on virtual asset activities where they are detected.

Investigators should frame their requests to the FIU in operational terms, explaining what they are looking for and why, rather than asking for “all information” on a subject. They should also indicate time sensitivity and known links to high-risk sectors, NPOs, or geographic areas.

Practical FIU–LEA Cooperation Model

A practical cooperation model can include the following steps:

- The investigative authority submits a targeted request to the FIU, clearly describing the case and the operational questions;
- The FIU applies a risk-based approach to prioritise the case;
- The FIU prepares analytical products, including data extracts, pattern analysis, and network diagrams;



- A joint meeting is held to interpret anomalies and key findings and to agree on investigative follow up and possible needs for additional FIU analysis;
- Investigators conduct fieldwork, interviews, surveillance, or searches based on the FIU's analysis and share feedback on the usefulness of the products; and
- Prosecutors and investigators integrate FIU findings into the evidentiary and asset recovery strategy and consider whether information is relevant for domestic or international targeted financial sanctions processes.

Why this matters?

FIU analysis reveals patterns, relationships, and anomalies that are invisible from police records alone. Structured cooperation avoids duplication, speeds up the investigation, and strengthens both intelligence and evidence. It also improves the quality of STR feedback and reinforces the risk-based approach of reporting entities.

5.8 Investigative Techniques and Tools for TF Cases

Terrorist financing investigations use a set of techniques tailored to low value, repetitive, often digital and cross border financial behaviour. This section sets out key tools that investigators should use to transform raw data into actionable intelligence and evidence. A more hands on approach with concrete steps increases the ability of mid-level investigators to apply these techniques in practice.

Financial Flow Analysis

Investigators should map financial flows:

- From diaspora communities to individuals or entities in the country;
- From the country to conflict zones or high-risk jurisdictions; and
- Between small businesses, exchange offices, and personal accounts.

They should identify patterns such as structuring, circular transfers, “pass through” accounts, and flows that coincide with travel, meetings, or events. Particular attention should be paid to small but repeated transfers, especially when combined with ideological or operational indicators. In practice, investigators should obtain complete account statements, group transactions by counterparties, look for clusters of transfers around key dates, and visually represent flows using link charts to identify central nodes and unexplained intermediaries.

Digital and Virtual Asset Forensics

Investigators should identify and analyse:

- Mobile payment applications and digital wallets;
- Peer to peer transfer platforms;
- Virtual asset exchanges and over the counter brokers; and
- Evidence of conversion between cash, bank deposits, and virtual assets.

Digital forensics teams should examine devices for wallet applications, seed phrases, QR codes, and transaction records. Requests to virtual asset service providers may be required, using international cooperation mechanisms where necessary.



Investigators should document all identified wallet addresses, check them against available blockchain analytics tools or services, and correlate digital asset movements with known periods of travel, online activity, or operational preparation.

Open Source and Communications Correlation

Financial activity should be correlated with:

- Open-source information, including social media content, public fundraising campaigns, and propaganda material;
- Encrypted messaging patterns, such as the timing and intensity of communications; and
- Online activity linked to humanitarian, religious, or ideological narratives that may serve as a cover.

Investigators should look for overlaps between online campaigns and financial transfers, including the identities or aliases of organisers, donors, and beneficiaries. They should preserve relevant online content as evidence, identify key profiles repeatedly involved in fundraising or coordination, and compare them with customer data from financial institutions and telecom providers.

Transport, Travel, and Logistics Correlation

Financial data should be cross checked against:

- Ticket purchases and travel bookings;
- Border crossing records and passenger manifests;
- Vehicle rentals and fuel purchases; and
- Accommodation payments and safe house expenses.

Correlating these data sets helps identify how funds support physical movement, meetings, and operational preparation. Investigators should build timelines that show transactions and movements together, identify who paid for travel and accommodation, and check whether apparently unrelated third parties are repeatedly involved in paying for logistics linked to high-risk individuals.

Why this matters?

Using these techniques allows investigators to see how money, people, communication, and logistics interact. Without them, terrorist financing investigations remain superficial and miss critical parts of the network. A practical, step by step approach makes these tools usable even in environments with limited specialised resources.



5.9 Task Force Model for TF Investigations

Terrorist financing cases naturally cut across institutional boundaries. A task force model formalises cooperation and creates a single operational framework for complex cases. It is particularly useful in jurisdictions with fragmented competences or multiple security and judicial actors.

A terrorist financing task force can include:

- A lead investigative agency responsible for coordination;
- The FIU as a permanent analytical partner;
- A specialised terrorism and terrorist financing prosecutor;
- National security and intelligence service representatives;
- Customs and border officials, including cash courier units;
- Cybercrime and digital forensics specialists;
- Tax and revenue service representatives; and
- Liaison officers from key financial institutions where appropriate.

The task force should have a clear mandate, agreed procedures for information sharing, and regular joint case reviews. It should also maintain a common operating picture that is accessible to core participants, including summaries of ongoing cases, key risks, and priority targets.

Why this matters?

A task force model reduces fragmentation and ensures that all relevant factors contribute their data, expertise, and tools. This improves the quality and speed of investigations and reduces the risk that critical information will be overlooked. It also supports coherent messaging to political authorities and international partners.

5.11 Asset Tracing, Freezing and Confiscation

Asset tracking and confiscation are central to effective terrorist financing investigations. They aim not only to punish but also to prevent, by removing the resources that enable terrorist activity. Asset related measures should be closely coordinated with operational, intelligence, and sanctions related actions.

Key Principle

Asset recovery planning must begin at the start of the investigation, not at the end. Investigators should treat every significant financial lead as a potential route to an asset that can be restrained or confiscated. They should also consider whether the same information is relevant for targeted financial sanctions or designation proposals under national and international frameworks.



Operational Steps

Investigators and prosecutors should:

- Identify all assets, accounts, and financial instruments linked to suspects, facilitators, and related entities;
- Map beneficial ownership and control structures, including nominees and front companies;
- Trace the movement of funds domestically and internationally, identifying layering and integration steps;
- Detect informal transfer methods, such as unregistered value transfer systems, unrecorded cash movements, and unregistered money remitters;
- Identify unexplained wealth by comparing assets and expenditure with lawful income;
- Recommend early temporary freezing or restraint orders where the legal threshold is met;
- Document legitimate income carefully so that discrepancies can be demonstrated in court;
- Prepare a confiscation strategy, including legal grounds, evidentiary needs, and international cooperation requirements; and
- Target assets held by facilitators and intermediaries, not only those in the name of primary suspects.

Why this matters?

Effective asset tracking and confiscation disrupt terrorist financing at its core. They prevent the reuse of funds, reduce the capacity of networks to reorganise, and provide a visible measure of success to domestic authorities and international partners. They also demonstrate that the jurisdiction uses all available legal tools in a coordinated way.

5.10 Operational Checklists

Checklists provide a simple way to ensure that key steps are not missed. They are particularly useful for standardizing practice across different units and for training new investigators and prosecutors. They also make it easier to document and review whether a case has been handled in line with national guidance.

Investigator Checklist

For every terrorist financing case, investigators should verify that they have:

- Launched a parallel financial investigation;
- Requested and received FIU analytical products;
- Identified and mapped all banking and MVTs channels;
- Analysed remittance patterns, including diaspora related flows;
- Assessed potential NPO involvement and carried out basic due diligence on relevant organisations;
- Checked for virtual asset and digital wallet activity;
- Conducted a lifestyle and income comparison;
- Examined cash courier and cross border cash movement data; and



- Prepared a recommendation for freezing or restraint of assets where appropriate.

Prosecutor Checklist

Prosecutors should verify that they have:

- Issued timely orders for financial, telecommunications, and digital data;
- Reviewed key financial indicators and FIU analysis;
- Coordinated directly with the FIU on analytical questions;
- Initiated planning for freezing and confiscation of assets;
- Ensured that facilitators and intermediaries are addressed in the case theory; and
- Monitored the progress of parallel investigations to maintain coherence.

Why this matters?

Operational checklists increase consistency, reduce the risk of omissions, and make it easier to demonstrate to evaluators that a systematic approach is in place. They also support internal quality control, on the job training, and institutional memory in units with staff turnover.

5.13 Rapid Triage Table for TF Indicators

Rapid triage tools help investigators quickly identify which financial behaviours require immediate attention and more detailed analysis. This is especially important in terrorist financing cases, where individual transactions may be small but collectively significant. A simple table encourages investigators to think in terms of categories, indicators, and immediate actions.

Rapid triage tools help investigators quickly identify which financial behaviours require immediate attention and more detailed analysis. This is especially important in terrorist financing cases, where individual transactions may be small but collectively significant.

Category	TF indicators	Immediate actions
Cash activity	Small, repetitive deposits; informal cash collections; no clear link to income	Obtain bank records; conduct lifestyle analysis; request FIU support
Remittances	Multiple senders; clustering in time or geography; vague or identical payment references	Profile senders; interview key senders or recipients; review relevant STRs
NPO links	Cash based operations; foreign donors; weak governance; no clear program activity	Conduct financial analysis; perform site visit; review NPO registration and reporting
Returnee links	Donations or transfers around travel dates; support from unknown donors; third party payments	Map social and financial networks; plan surveillance or interviews
Virtual assets	P2P transfers; sudden wallet activation; frequent small	Send requests to VA service providers; perform device



	conversions between cash, bank, and VA	forensics; review FIU VA intelligence
--	---	--

Why this matters?

A simple triage table allows investigators to focus resources on the most relevant and risky behaviours. It speeds up decision making and helps ensure that critical early opportunities are not missed. It also provides a transparent structure for supervisory and judicial review of investigative priorities.



6. Chapter Six - Sources of information for identifying and investigating terrorist financing

6.1 Financial Intelligence Unit (FIU) and Suspicion Transaction Reports (STRs)

STRs are a critical entry point for uncovering terrorist financing, especially in cases where conventional investigative methods may not detect covert financial flows. To use STRs effectively, practitioners should follow a structured, multi-source approach. For example:

6.1.1 Early Coordination with the FIU:

- Initiate contact with the FIU as soon as a terrorism-related STR is flagged.
 - Gain access to linked STRs, additional financial intelligence, and cross-border alerts.
 - An STR showing repeated small transfers from a high-risk jurisdiction may be part of a broader network. The FIU can provide related reports from other institutions or jurisdictions
- Prioritizing High-Risk STRs

6.1.2 Prioritizing High-Risk STRs:

- Use risk indicators to triage STRs (prioritize those involving:
- Transfers from conflict zones
- Use of cash-intensive services (e.g., Western Union)
- Links to NGOs with opaque funding
- For example, an STR involving a small NGO receiving frequent foreign donations followed by cash withdrawals should be flagged for immediate review.

6.1.3 Analysing Transaction Data:

- Examine transaction patterns for signs of layering or structuring:
- Multiple small deposits (smurfing)
- Rapid fund movement across accounts or borders
- Use of third-party accounts
- Evidence Sources: Bank logs, remittance records, MTO data, and STR metadata.
- For example, a suspect receives €500 transfers weekly from different senders in Germany, all using similar remittance agents.

6.1.4 Linking Customer Identification with External Records

- Cross-reference STR identity data (name, ID, nationality) with border crossing logs, immigration databases and telecom metadata
- For Example, a person flagged in an STR for unexplained cash deposits is found to have travelled multiple times to Türkiye and Syria, aligning with known TF routes.

6.1.5 Connecting Behavioural Red Flags with Communication Data



- Use the STR narrative to identify behavioural anomalies (e.g., evasiveness, inconsistent explanations).
- Request call detail records (CDRs), social media activity, or encrypted messaging logs.
- For example, a customer cited for reluctance to provide documentation is later found communicating with known extremist contacts via secure messaging apps.

6.1.6 Asset Tracing and Property Linkage

- Match financial flows with asset purchases or holdings: real estate, vehicles and high-value goods
- Sources could include customs declarations and tax filings.
- For example, funds flagged in an STR are traced to a property purchase under a relative's name, with no declared income.

6.1.7 Building a Multi-Source Intelligence Picture

- Integrate STRs with open-source intelligence, human intelligence, and FIU exchanges

An example could be an STR narrative mentions donations to a charity later identified in UN sanctions lists; OSINT confirms ideological alignment with extremist causes.

The Financial Intelligence Department operates under the AML CFT Law of BiH as the central body responsible for preventing, analysing, investigating, detecting and combating money laundering, associated predicate offences and terrorist financing. It receives, collects, records, analyses and investigates financial information and forwards the results of its analytical and investigative work to competent domestic authorities and to competent bodies of other countries. The Department functions autonomously and operationally independently within the structure of SIPA and makes its own decisions regarding the processing and dissemination of information. It performs tasks that are separate from those of other organisational units, supported by appropriate staffing, technical capacity and restricted access to sensitive financial data. It operates with free decision making when handling information and conducting its analytical or investigative work, and it may request support from other SIPA units when necessary to perform tasks prescribed by the Law.

Under the AML CFT Law, the Department receives suspicious transaction reports on money laundering and terrorist financing, cash transaction reports, reports on attempted transactions and all other reports that obliged entities are required to submit. It is authorised to request additional information from obliged entities, supervisory bodies and competent institutions whenever it is necessary for its analytical or investigative work. It may collect information from public authorities and private bodies to clarify the origin, purpose and movement of funds. It also cooperates and exchanges information with foreign financial intelligence units and international organisations involved in combating money laundering and terrorist financing.



The Financial Intelligence Department is required by the AML CFT Law to submit a formal report to the competent prosecutors office whenever it determines that there are grounds to suspect the criminal offence of terrorist financing. When it temporarily suspends a transaction that may relate to terrorist financing and considers that a court order is needed for an extension, it must immediately inform the competent prosecutor. If the Department identifies information that may assist prosecutors or law enforcement agencies in decisions that fall within their investigative powers, it must notify them in writing and provide all relevant data and documentation. The Department must also inform competent authorities if, during its work, it uncovers indications of other criminal offences connected with terrorist financing. When sending notifications or reports, the Department must respect subject matter and territorial jurisdiction and direct its information to the correct authority.

Prosecutors and other competent authorities may request financial intelligence from the Department, and the Department must provide all available information that can support investigations related to terrorist financing, provided that the request meets the legal requirements. The Department independently determines the procedure and scope of checks it will conduct when acting on such requests. It may reject requests that do not contain the required legal basis, identification data, description of the suspicion and urgency level, and it must inform the requesting authority in writing when this occurs. The Department is not obligated to provide information if doing so would jeopardise an ongoing investigation or if disclosure would be clearly disproportionate or irrelevant, and it must document the reasons for such a decision. When forwarding information to competent authorities, the Department may prohibit the further sharing of that information without its prior written consent.

6.2 Operational meaning for TF investigations

For terrorist financing investigations, these provisions mean that financial intelligence from the FIU is an immediate trigger for prosecutorial action. When the FIU identifies grounds to suspect terrorist financing, it must proactively notify the competent prosecutor and provide the analytical and investigative material necessary to open a case. Notifications concerning temporarily suspended transactions allow prosecutors to quickly seek court orders and prevent the movement of funds linked to TF activity. Written intelligence produced by the FIU gives investigators a factual basis to map financial flows, identify support networks and plan early operational steps.

Prosecutors must ensure that requests to the FIU are specific and legally grounded, after which the FIU is obliged to provide all relevant information. The FIU may restrict the further sharing of its intelligence, so investigators must respect confidentiality requirements and use the information only within authorised limits. Prosecutors are also required to inform the FIU about the results achieved using the financial intelligence to maintain effective cooperation. Since the FIU can decline to provide information if disclosure would compromise its ongoing analytical or investigative work, early communication and clear coordination are essential for timely and effective TF investigations.



Table 1: Checklist for Requesting Information from the FIU (TF Cases)

What to Verify	What to Include	How to Follow Up
Confirm relevance to a suspected TF offence	Legal basis for the request	Be ready to provide clarifications to the FIU
Check whether the FIU already sent a report on the same subjects	Full identification data of persons or entities	Integrate FIU intelligence into investigative planning
Ensure the request falls within your institutional competence	Description of the TF suspicion with factual elements	Respect any FIU restrictions on further dissemination
Make sure internal approvals are completed	Specific information or documents requested	Document how FIU intelligence was used in the case
Avoid broad or unfocused requests	Justification of urgency	Provide mandatory feedback to the FIU on results

Table 2: Checklist for Acting on FIU Notifications (Article 70 Situations)

Upon Receiving FIU Notification	Key Actions to Take	Follow-Up Requirements
Treat the FIU notification as legal grounds to assess opening a TF case	Review all data and analysis provided by the FIU	Inform the FIU of investigative results as required by law
Verify subject matter and territorial jurisdiction	Secure financial records, account statements and related documentation	Maintain confidentiality and respect any FIU limits on sharing
Assess urgency, especially in cases involving suspended transactions	Coordinate with the prosecutor to request court orders when needed	Update operational plans based on new FIU intelligence
Identify financial flows, facilitators or networks	Initiate tracing, interview planning and other early investigative steps	Provide structured feedback to the FIU for continuous cooperation
Check whether parallel investigations are ongoing	Ensure measures are taken quickly to prevent dissipation of funds	Document all actions triggered by the FIU notification

6.3 Banking data and KYC documentation (financial sector)

Investigators should request KYC files directly from reporting entities (e.g., banks, money transfer operators) via formal written requests or court orders, depending on the stage of the



investigation. Early coordination is crucial to ensure that requests are targeted and legally compliant.

Practical Guidance for Investigators

- Initiate a KYC Request Promptly
- Upon receiving an STR or identifying a high-risk transaction, investigators should submit a formal request to the relevant financial institution for the full KYC file. This would include account opening forms, copies of identification documents, source of funds declarations, customer risk assessments, records of communication or internal compliance notes

Example 1

- An STR indicates that an individual received multiple €500 transfers via Western Union from Germany. Investigators request the KYC file from the remittance provider, revealing that the recipient used a foreign passport with no local address and declared 'personal gift' as the purpose of each transaction. This raises red flags when cross-referenced with travel records showing frequent trips to Türkiye and the Middle East.
- Cross-Reference with External Databases
- Once obtained, KYC data should be checked against - sanctions lists (e.g., UN, EU, OFAC), PEP databases (e.g., World-Check, Dow Jones), domestic watchlists, international cooperation channels (e.g., INTERPOL, Egmont Group)

Example 2:

- A customer's declared occupation is "import-export agent," but the KYC file lacks any supporting documentation. A check against INTERPOL notices reveals the individual is under investigation in another jurisdiction for financing foreign terrorist fighters.
- Use KYC to map networks, KYC records often include information on linked accounts, authorised signatories, or business partners. Investigators should use this to map potential facilitators or shell entities.

Example 3:

- A small NGO flagged for suspicious cash withdrawals lists a board member who is also a signatory on another account receiving funds from the same foreign donor. This connection may indicate a coordinated terrorist financing network.

Preserve chain of custody, all KYC documents obtained should be logged and stored in accordance with evidentiary standards to ensure admissibility in court. Investigators should document the request process, receipt, and any analysis conducted.

Financial institutions are required by the AML CFT Law to identify and verify their customers before establishing a business relationship and to collect the full set of KYC documentation prescribed by the Law. They must keep all customer identity data, account files and



transaction records for a period of at least ten years and make them available to the FIU upon request for the purpose of analysing suspected money laundering or terrorist financing. Banks are obliged to maintain accurate and up to date information on beneficial ownership and to submit suspicious transaction reports together with supporting KYC and account documentation. All customer and transaction data held by financial institutions must be provided to competent authorities when required for the investigation of money laundering, associated predicate offences or terrorist financing.

Prosecutors and investigators use bank account data and KYC files to verify the identity, financial profile and transaction behaviour of persons connected to suspected TF activity. These records help establish whether the customer's declared income and background correspond to the financial movements detected during the investigation. KYC documentation is essential for identifying beneficial owners, tracing linked accounts and uncovering hidden networks or facilitators supporting the suspect. Transaction histories allow investigators to map the flow of funds, detect patterns of structuring and identify transfers that lead to foreign or domestic TF channels. Banks' internal notes, risk assessments and explanations for unusual activity provide additional context that helps prosecutors build a clear and defensible financial narrative in TF cases.

What Banks Hold	How Investigators Use It in TF Cases
Customer identification data and verified KYC documents	Confirm the identity, background and financial profile of suspects and associated persons
Beneficial ownership information	Identify hidden owners, linked persons and structures used to conceal TF activity
Account statements, transaction histories and transfer details	Map the flow of funds, detect suspicious patterns and identify domestic or cross-border TF channels
Records of cash deposits, withdrawals and currency exchanges	Analyse unexplained cash activity, structuring and possible use of alternative value-transfer systems
Internal bank notes, risk assessments and explanations for unusual transactions	Understand the context of suspicious activity, identify red flags and strengthen the evidentiary basis for TF charges

6.4 NPO sector and specific activity reports

The charity sector can provide valuable sources of information for identifying and investigating terrorist financing. Financial records can reveal suspicious patterns including frequent transfers to high-risk jurisdictions and unexplained cash withdrawals. These could indicate fund diversion or abuse of charitable structures. Regulatory filings, such as annual reports and submissions to a charity regulator could provide transparency on income, expenditure, and programmatic activities. Discrepancies between declared missions and actual operations, especially in conflict zones or areas with limited oversight, could signal misuse.



The charity and non-profit sector present both opportunities and risks in the context of terrorist financing. While many NPOs provide essential services, certain structural and oversight weaknesses make them susceptible to exploitation. This is especially true for:

6.4.1 High-Risk NPO Types:

- Small religious charities with opaque governance structures and limited financial transparency.
- Humanitarian aid organizations operating in or near conflict zones (e.g., Syria, Türkiye, Gaza), often receiving foreign donations.
- Diaspora-linked NPOs that channel funds from expatriate communities abroad, sometimes with minimal documentation.
- Unregistered or loosely regulated associations, including informal community groups that solicit donations without formal oversight.

6.4.2 Investigative Use of Financial and Regulatory Data:

LEAs and prosecutors could strengthen terrorist financing investigations by analysing the following data sources:

Financial Records:

- Bank statements and transaction logs can reveal:
 - Frequent transfers to high-risk jurisdictions (e.g., Türkiye, Lebanon, Pakistan)
- Unexplained cash withdrawals shortly after receiving foreign donations
- Use of personal accounts for NGO-related transactions

Example 1

A charity receives €20,000 from a donor in Austria, followed by multiple cash withdrawals and transfers to an account in Gaziantep, Türkiye.

Regulatory Filings:

- Annual reports, programmatic declarations, and financial disclosures submitted to the Ministry of Justice or relevant cantonal authorities can be used to:
 - Compare declared missions with actual spending
- Identify inconsistencies in income vs. expenditure
- Detect missing or falsified documentation

Example 2

An NGO declares its mission as “local youth education” but reports €15,000 in travel expenses to Jordan and no local programming.



Donor and Beneficiary Data

- Donor lists and correspondence can help trace ideological or geographic links to high-risk networks.
- Beneficiary records may reveal overlaps with sanctioned individuals or entities.

Example 3

A charity's donor list includes individuals flagged in EU or UN sanctions databases, and its beneficiaries include persons under investigation for radicalisation.

Cross-Referencing with STRs and KYC Data

- Match NGO account activity with Suspicious Transaction Reports (STRs) and Know Your Customer (KYC) files from banks and remittance services.

Example 4

A small NGO flagged in an STR for frequent Western Union pickups is found to share board members with another entity under investigation for TF.

Recommendations:

- Coordinate access STRs and financial intelligence.
- Use open-source intelligence to monitor social media, websites, and fundraising campaigns.
- Engage with charity regulators and tax authorities to obtain filings and audit reports.

Apply forensic accounting techniques to reconstruct fund flows and identify layering or diversion.

6.5 Customs and border services

Customs authorities collect and analyse a wide range of data that can reveal indicators of terrorist financing. Unusual patterns could include frequent declarations below reporting thresholds or undeclared bulk cash. Trade documentation, such as invoices, bills of lading, and customs declarations, may expose trade-based terrorist financing schemes, where goods are mispriced, misclassified, or falsely documented to disguise fund transfers. Border services can collect passenger and cargo data. These can identify individuals or entities with links to high-risk jurisdictions or known terrorist networks.

6.6 Open sources (media, social networks, blockchain analytics)

Open-source intelligence has the potential to become an increasingly important in CTF efforts. Media reports can reveal early indicators of terrorist activities and related investigations can also expose abuse of humanitarian aid, trade-based schemes, or crypto fundraising campaigns.



Social networking platforms are frequently used by terrorist groups for propaganda, recruitment, and fundraising. Analysts could monitor such platforms for appeals to donate, cryptocurrency wallet addresses, or links to crowdfunding campaigns. Blockchain analytics offers an interesting tool for tracing terrorist financing through cryptocurrencies. Despite the pseudonymous nature of blockchain transactions, tools like Chainalysis can identify wallet addresses associated with terrorist entities, track fund flows across exchanges, and detect mixing or obfuscation techniques.

6.7 International cooperation and intelligence channels (Egmont, Europol, Interpol)

The Egmont Group connects over 170 FIUs enabling a secure and confidential exchange of STRs. The Egmont Secure Web enables FIUs to request and share information on cross-border fund flows, beneficial ownership, and links to designated terrorist entities. Egmont also publishes sanitized case studies and typology reports which could assist identify emerging terrorist financing methods.

Europol, through its European Financial and Economic Crime Centre and the Terrorist Financing Tracking Programme, provides operational support to EU Member States. Europol enables joint investigations and real-time intelligence sharing, using SIENA to exchange data on suspects, transactions and crypto wallets, and combining open-source and blockchain analytics to trace fundraising via social media and crowdfunding.

INTERPOL advances global counter-terrorist financing through its Financial Crime and Anti-Corruption Centre, maintaining databases on stolen and lost travel documents, wanted individuals, and financial-crime suspects. Its network allows member countries issue alerts and rapidly shares intelligence on terrorist financiers, including those using trade-based schemes, illicit commodity flows, or digital currencies. INTERPOL also works with FATF and other international bodies to align policy and operational priorities.

International cooperation is a core element of BiH's ability to detect, analyse and disrupt cross-border terrorist financing activities. The FIU of BiH exchanges financial intelligence primarily through the Egmont Secure Web, which enables direct communication with foreign FIUs. During the recent assessment period, the FIU processed dozens of requests and spontaneous information from foreign FIUs related to suspected terrorist financing, including cases linked to foreign terrorist fighters, humanitarian organisations and cross-border money transfers. The AML CFT Law provides a sufficient legal basis for the FIU to exchange information spontaneously or upon request with foreign FIUs and foreign law enforcement bodies without the need for additional bilateral agreements, although BiH FIU has signed several Moues when required by partners.

BiH relies on INTERPOL channels for information exchange, identification of persons of interest, and assistance in cases involving extradition or the tracing of internationally mobile suspects. INTERPOL provides access to databases containing information on wanted persons, forged documents, fingerprints and travel patterns. The INTERPOL National Central Bureau in BiH supports terrorism financing investigations by coordinating international alerts, including notices related to foreign terrorist fighters and facilitators. Although INTERPOL



does not conduct investigations, it provides essential operational coordination and helps BiH authorities identify associates, movement patterns and possible financial links of TF suspects.

Europol is an increasingly important channel for BiH law enforcement in TF-related cases, particularly through SIENA, Europol's secure information exchange system. BiH authorities have processed Europol requests related to foreign terrorist fighter lists, cross-border transfers and bank transactions linked to persons with TF risk indicators. Through Europol, BiH investigators also obtain analytical products, intelligence leads and information that support ongoing TF cases. Cooperation between the FIU and Europol is indirect but functional, especially when FIU information is required to validate data received through Europol channels.

These intelligence channels complement each other. Egmont provides financial intelligence, INTERPOL covers identity and movement information, while Europol supports broader operational intelligence and analytical products. Efficient use of all three channels enables prosecutors and law enforcement agencies in BiH to follow financial trails across borders, identify networks, and coordinate actions with foreign partners in real time.

Channel	What it provides?	How BiH uses it in TF cases
Egmont FIU to FIU	Financial intelligence, bank data, STRs, cross border financial flows, information on NPOs, remittances and money transfers	FIU BiH requests and exchanges financial intelligence regarding foreign terrorist fighters, humanitarian associations, informal transfer channels and cross border transactions. FIU receives spontaneous information and sends replies to foreign FIUs for verification of domestic bank transactions, identities and associated persons.
Europol (SIENA)	Operational police intelligence, analytical reports, links between suspects, phone data, travel patterns, FTF lists, risk analysis	BiH LEAs use Europol information to identify connections between domestic subjects and foreign TF networks, verify whether BiH nationals travelled to conflict zones, and trace suspicious international transactions. Europol analytical products support prosecutors in



		building transnational TF cases.
Interpol	Global police databases, Red Notices, identity checks, fingerprints, travel documents, vehicle data, alerts	BiH authorities use Interpol to locate TF suspects, verify identities, trace movement across borders, and obtain criminal history or alerts from other jurisdictions. Interpol supports extradition, liaison coordination and urgent communication in TF investigations.

6.8 Additional and Emerging Sources of Information

Consider integrating the following additional and emerging sources of information relevant to terrorist financing investigations, particularly in light of evolving typologies and digital platforms:

6.8.1 Virtual Asset Service Providers and Blockchain Analytics

- Terrorist groups increasingly exploit cryptocurrencies for cross-border transfers, fundraising, and value storage.
- Sources of information: VASP compliance reports and transaction logs, Blockchain analytics tools (e.g., Chainalysis, TRM Labs), wallet tracing and clustering techniques
- Use case: Linking pseudonymous wallets to known TF suspects or identifying donation campaigns using privacy coins.

6.8.2 Online Crowdfunding and Social Media Platforms

- Extremist actors use platforms like GoFundMe, Telegram, and Facebook to solicit donations under humanitarian or ideological covers.
- Sources of information: Platform takedown reports, payment processor records, open-source intelligence from campaign pages and donor comments
- Use case: Identifying campaigns that redirect funds to conflict zones or sanctioned entities.

6.8.3 Online Gaming Ecosystems and In-Game Economies

- Some terrorist financiers exploit in-game currencies and digital assets to move value covertly.
- Sources of information: • game platform transaction logs, account registration and IP metadata, reports from gaming companies and cybersecurity firms



- Use case: Detecting laundering through virtual goods or peer-to-peer trades in multiplayer games.

6.8.4 Threat Intelligence Feeds and Cybercrime Indicators

- Terrorist Financing networks often overlap with cybercrime infrastructure (e.g., phishing, ransomware, shell companies).
- Sources of information: commercial threat intelligence platforms, indicators of compromise linked to financial fraud, dark web monitoring
- Use case: Mapping TF facilitators who also engage in cyber-enabled financial crime.

6.8.5 Natural Resource Trade and Commodity Flows

- Terrorist groups have funded operations through illicit trade in gold, charcoal, oil, and narcotics (e.g., Captagon).
- Sources of information: Customs seizure data, trade anomaly reports (undervaluation, false invoicing), satellite imagery and NGO field reports
- Use case: Tracing TF-linked supply chains or front companies involved in resource extraction.

6.8.6 Tax Authority and Business Registry Data

- Shell companies and front entities are often registered with minimal oversight.
- Sources of information: corporate registries, tax filings and VAT records, beneficial ownership declarations
- • Use case: Identifying dormant or suspicious entities linked to TF suspects or NPO abuse.

6.8.7 Diaspora and Remittance Network Mapping

- Remittance corridors from diaspora communities can be exploited for TF, especially via informal channels.
- Sources of information: MTO transaction data, community association records, travel and migration databases

Use case: Profiling high-risk remittance flows and identifying intermediaries.



7. Chapter Seven - Best practices and patterns in identifying terrorist financing

7.1 Introduction

This section outlines practical best practices for disrupting terrorist financing, centred on a follow the money methodology that traces transactional flows to reveal networks and intent, and will illustrate these approaches with targeted case studies; it emphasises the creation of multidisciplinary teams and joint investigation groups that bring together financial investigators, prosecutors, law enforcement, intelligence and regulatory specialists, the immediate use of rapid temporary prohibitions on asset disposal to prevent dissipation, and the deployment of specialised financial analysis. This includes transaction pattern analysis, trade-based scrutiny, virtual asset tracking and beneficiary mapping, all supported by seamless coordination among police, prosecution, FIUs and other competent authorities to enable timely intelligence exchange, preserve evidence and increase the likelihood of successful disruption and prosecution.

Case Study 1 – Successful use of Financial Investigations for Terrorist Financing:

Amal El-Wahabi was convicted under the Terrorism Act for arranging a €20,000 transfer to her husband fighting for ISIL in Syria, after financial, travel and communications intelligence revealed her role and intent. The NTFIU, Border Force, security services and overseas law enforcement used Passenger Name Record data (personal and travel information gathered by airlines and travel agents when a booking is made) call-detail records and real-time intelligence to trace the cash courier, intercept the funds at the airport, and forfeit the money as terrorist property; El-Wahabi received a 28-month sentence while the courier was acquitted. The case highlights how multi-agency data fusion, linking financial, travel and telecoms records, can effectively disrupt terrorist financing when information-sharing mechanisms are in place.

Case Study 2 – Successful use of Financial Investigations for Terrorist Financing:

The conviction of London art dealer Oghenochuko Ojiri demonstrates the power of financial intelligence in combating terrorist financing: between Oct 2020 and Dec 2021 he sold £140,000 of art to Nazem Ahmad, a sanctioned individual linked to Hezbollah but deliberately failed to report the transactions and concealed Ahmad's identity with altered invoices and deceptive WhatsApp messages. Investigators used transaction records, regulatory oversight and phone evidence to show he knew the legal obligations under the Terrorism Act 2000 and wilfully ignored them, leading to a landmark prosecution. The case sets a legal precedent for enforcing anti-money-laundering and sanctions rules in the art market and highlights how financial investigation, data analysis and interagency cooperation can detect, disrupt and deter terrorism financing.



Case Study 3 – Success of Financial Investigations – Joint Money Laundering Intelligence Task Force

The Joint Money Laundering Intelligence Taskforce (JMLIT) is a public-private partnership formed to tackle high-end money laundering by sharing strategic, tactical and operational intelligence between law enforcement and the financial sector. Launched in 2015, it brings together over 200 members including banks, the FCA, NCA, HMRC, SFO, City of London Police and the Met, and has rapidly advanced voluntary information sharing and response. By the end of 2024 JMLIT helped identify more than 10,700 previously unknown accounts (over 8,100 closed), contributed to about 400 arrests, supported roughly 1,230 legislative orders, put over £248 million under restraint and issued 100 sector alerts. International bodies and jurisdictions — including FATF, Australia, Singapore and Hong Kong — cite JMLIT as an innovative model and best practice for public-private data sharing to disrupt illicit finance

Case Study 4 – Joint Fraud Task Force

The Joint Fraud Taskforce (JFTF) is a public-private partnership uniting government, law enforcement and the financial sector to tackle complex frauds that no single organisation can manage alone. It provides a coordinated fraud strategy, oversight of implementation, strategic threat analysis, data sharing and victim-reduction activity, and fosters industry collaboration. Its flagship Data Fusion initiative, led by the NCA, pooled voluntary bank transaction and customer data with organised-crime datasets in a pilot (Oct 2021–Feb 2022), producing about 90 intelligence packages, identifying previously unknown organised-crime networks, improving high-priority investigations and helping banks strengthen counter-fraud controls. In July 2025, the Home Office-made Data Fusion a permanent operational capability, including a permanent public-private Joint Analytical Team within the NCA, institutionalising the JFTF's cohesive, cross-sector approach to disrupting fraud.



7.2 Investigative techniques and tools

Terrorist financing investigations require a multi-layered approach that combines financial intelligence, digital forensics, covert operations, and international cooperation. This section provides suggested guidance for LEAs and investigators to trace illicit financial flows, uncover digital evidence, and disrupt terrorist networks.

7.2.1 Financial Flow Analysis

- Use STRs and CTRs: Obtain STRs from the FIU and prioritize those involving high-risk jurisdictions, cash-intensive activity, or NGO-linked accounts.
- Review CTRs for large or structured cash deposits that may indicate smurfing or layering.
- Coordinate Early with the FIU: request aggregated data and analytical support.
- Use FIU platforms to identify linked entities and cross-border patterns.
- For example, an STR shows repeated €500 transfers from Germany to a Bosnian NGO. FIU analysis reveals similar patterns across multiple NGOs with shared board members.

7.2.2 Digital Forensics and Cryptocurrency Tracing

- Deploy Blockchain Analytics Tools: use platforms like Chainalysis or TRM Labs to trace wallet activity, identify mixers, and monitor exchange flows.
- Flag wallets receiving donations from extremist-linked campaigns or forums.
- Examine Seized Devices and Wallets: secure judicial warrants to access mobile phones, laptops, and hardware wallets.
- Extract metadata, IP logs, and timestamps to link virtual assets to suspects
- For example, a suspect's phone contains a wallet app linked to a donation address promoted on a Telegram channel supporting foreign terrorist fighters.

7.2.3 Dark Web and Online Platform Monitoring

- Monitor Crypto Fundraising and Procurement Channels: track extremist forums, encrypted messaging apps, and crowdfunding platforms.
- Identify campaigns using humanitarian covers to solicit funds.
- Use open-source intelligence and cyber threat intelligence: use commercial feeds and dark web monitoring tools to detect terrorist financing related activity.
- For example, a fundraising page claims to support “medical aid in Syria” but is linked to a wallet previously flagged in Europol's TF database.



7.2.4 Screening and International Databases

- Screen Individuals and Entities Against:• UN, EU, and OFAC sanctions lists
- INTERPOL notices and Europol databases
- Domestic watchlists and PEP registries

7.2.5. Use of criminal intelligence techniques to detect terrorism financing schemes, channels as well as related people

Recommended criminal intelligence techniques that can be used in conjunction with financial intelligence tools:

1) covert human intelligence activity - means a method of collecting criminal intelligence through trusted covert participants of criminal intelligence and/or collaboration with other individuals.

2) inquiry -means a method of collecting criminal intelligence through direct communication with individuals possessing pertinent information. Secret inquiry means the type of inquiry where the affiliation of the inquiry officer with a criminal intelligence entity is concealed through encryption.

3) inspection - means a method of collecting and documenting criminal intelligence through public, encrypted or secret inspection of objects, documents, premises, vehicles, locations, persons or other items.

4) verification - means a method of collecting criminal intelligence by verifying the criminal intelligence received as well as by identifying the existence of items and/or services prohibited in circulation and procuring them.

5) controlled delivery -means an authorised method of collecting intelligence involving the controlled passage of goods and other items into, though, or out of the territory of the BiH, where the transport of these goods or items is unlawful or suspect and where this operation is conducted under the supervision of a criminal intelligence entity with a view to detecting criminal acts and identifying persons involved in, planning, or having committed such criminal acts.

6) simulation of a criminal act - means an organisational tactical approach within criminal intelligence activities, utilizing specific methods and tools to collect intelligence for the execution of designated criminal intelligence tasks.

7) ambush - means a method of collecting criminal intelligence, which is employed for impeding individuals involved in, planning or having committed a criminal act and for collecting pertinent information crucial for investigating the criminal act, where there is



actionable intelligence on the individuals involved and/or details on the location and timing of commission of the criminal act.

8) surveillance - means a method of collecting criminal intelligence by detecting, recognising and/or observing a criminal intelligence target.

9) undercover operation - means collecting criminal intelligence through engaging or otherwise involving covert participants of criminal intelligence and employees of criminal intelligence entities. This method shall be employed where there are grounds for conducting a criminal intelligence investigation.

7.2.6 Criminal intelligence entities, responsible for the detection and investigation of terrorism and terrorism financing shall be tasked to do the following:

- 1) prevent criminal acts;
- 2) detect criminal acts and identify the persons involved in, planning or having committed them;
- 3) search for items, money, securities, and other property associated with the commission of criminal acts.

7.2.7 Where information on criminal intelligence targets is available, criminal intelligence entities shall have the right to take the following steps:

- 1) to use methods of collecting criminal intelligence, where in view of the nature and/or duration of the use of the said methods no sanction from a prosecutor or a court is required;
- 2) to use technical means under standard procedure;
- 3) to establish contacts with persons who have become criminal intelligence targets;
- 4) to use the assistance of individuals for the implementation of criminal intelligence tasks;
- 5) to use expert help for the implementation of criminal intelligence tasks;
- 6) to covertly obtain fingerprints, human voice samples, human smell samples and other samples for investigation;
- 7) to use the documents required under the intelligence legend for conducting covert human intelligence activity against detainees detained or arrested in the course of covert human intelligence activity;
- 8) to monitor public information disseminated in the mass media.
- 9) to cooperate with foreign law enforcement institutions, international organisations, and



European Union agencies in the cases provided for by international treaties and legal acts of the BiH, provide mutual support, and exchange criminal intelligence and other information.

7.2.8 If grounds set out in legal acts regulating the use of tools for a criminal intelligence investigation appear and a sanction is obtained from a relevant authority; criminal intelligence entities shall have the following additional rights:

- 1) obtain data from undertakings providing electronic communications networks and/or services.
- 2) to use technical means under specialised procedures for conducting covert inspections of postal items and documents they contain, covert monitoring and confiscation of postal items, and covert oversight of correspondence and other communications.
- 3) to covertly enter a person's residence, official or other premises, enclosed areas, and vehicles, to conduct their inspection, retrieve documents, objects, samples, and other items essential for criminal intelligence, and examine and/or mark these items without formally declaring their confiscation.
- 4) to use the following methods of collecting criminal intelligence: controlled delivery, simulation of criminal acts and surveillance.



8. Chapter Eight - Summary and key recommendations

Key Recommendations to Improve Immediate Outcome 9

1. Strengthen the Financial Intelligence Unit

- Improve analytical capacity to detect terrorist financing specific patterns and distinguish TF from general money laundering.
- Enhance feedback mechanisms to reporting entities to improve STR quality and relevance.
- Invest in technology and staffing to support proactive intelligence generation and dissemination.

2. Prioritise TF Investigations and Prosecutions

- Develop terrorist financing specific investigative protocols and training for law enforcement and prosecutors.
- Track and report terrorist financing convictions separately from general money laundering statistics to demonstrate effectiveness.

3. Deepen Public-Private Partnerships

- Engage financial institutions and DNFBPs (e.g. accountants, lawyers, real estate agents) in TF typology sharing.
- Establish a national PPP platform modelled on JMLIT (UK) or EFIPPP (EU) to facilitate real-time intelligence exchange.
- Provide sector-specific guidance on terrorist financing risks, especially for non-profit organizations and fintechs.

4. Enhance Risk Understanding and Outreach

- Update the national terrorist financing risk assessment to reflect emerging threats.
- Conduct outreach to high-risk sectors, including NPOs and remittance providers, to raise awareness and improve compliance.
- Integrate TF risk indicators into supervisory and enforcement frameworks.

5. Improve Institutional Coordination

- Formalize inter-agency cooperation protocols between FIU, police, prosecutors, and intelligence services.
- Use joint task forces or fusion centres to coordinate TF investigations and share intelligence.
- Ensure timely and secure data sharing across agencies and with international partners.

6. Significantly improve capabilities in identifying and collecting information on terrorism and terrorist groups, as well as their financing channels and schemes, using criminal intelligence methods, including:

- develop the necessary internal instructions for the criminal intelligence officers on proper use of the criminal intelligence tools detecting terrorism related crimes, including terrorism financing.



- provide the necessary technical, financial, and human resources for the relevant units of law enforcement agencies for effective use of criminal intelligence tools.
- create special task forces to collect and share criminal intelligence information at the state and organizational levels.



9. Appendixes

APPENDIX 1

Operational Manual for Terrorist Financing Investigations

(Model for Countries with Similar Risk Profiles to Bosnia and Herzegovina)

1. Purpose

This manual provides a rapid, practical and operational overview of investigative steps and methods applicable to terrorist financing (TF) cases in jurisdictions characterised by high cash usage, active diasporas, informal money transfer channels, weak financial oversight over small organisations and fragmented security structures.

2. Key Characteristics of the TF Environment

Common characteristics in jurisdictions with this profile include:

- frequent small donations from diaspora individuals to one or more connected people
- cash withdrawals immediately after receiving transfers.
- informal fundraising activities
- use of third parties to send, receive or withdraw money.
- organisations operating in cash.
- purchase of digital assets using physical cash
- sudden sale of assets to finance travel
- closed circle social networks.
- parallel or inconsistent internal bookkeeping within organisations

These features represent high-risk indicators for TF and justify the initiation of a financial investigation.

3. FIRST 48 HOURS – OPERATIONAL CHECKLIST

(critical steps that must be taken immediately)

1. FIU urgent request
 - all STRs/CTRs
 - linked people.
-



- remittance/MTO logs
 - smurfing analytics
 - previous FIU inquiries from foreign jurisdictions
2. Telecommunication metadata
- time correlation between calls and transfers.
 - identification of central contacts
 - frequency of international communications
3. Travel pattern review.
- travel overlapping with receipt of donations.
 - one-way tickets
 - sudden or unexplained travel
4. KYC documentation
- consistency of income and expenditure
 - stated purpose of transactions.
 - information on donors
5. Digital review (OSINT + devices if available)
- public profiles
 - closed groups.
 - online ads showing urgent sales of assets.
 - evidence of crypto wallet applications
6. Rapid financial flow map (within 24 hours)
- who sends.
 - who receives.
 - who withdraws cash?
 - who transfers money further?
7. Contact the prosecutor.
- initial briefing
 - agreement on priorities



- requests for urgent orders

4. KEY TABLES AND DIAGRAMS

4.1. Table: STR → FIU → Prosecutor → Investigator

(the most important information flow)

Stage	Action	Key Output	Timing
1. STR/MTO indicator	Reporting entity files STR/CTR	initial trigger	immediate
2. FIU analysis	FIU connects flows, persons, remittances and digital traces	financial profile of subject	24–48h
3. FIU → Prosecutor	FIU provides urgent analytical information	basis for judicial orders	48–72h
4. Prosecutor → Investigator	Prosecutor issues orders based on FIU analysis	operational steps	72h+
5. Investigator → FIU	additional information returned to FIU	completion of intelligence picture	ongoing

4.2. Diagram: Basic TF Flow Model

(typical pattern of small, frequent TF transfers)

Diaspora (1–3 persons)

→ sends small transfers (100–500)

→ recipient withdraws cash the same day

→ intermediary holds or passes on the cash

→ subject uses funds for travel, logistics or further onward transfer.

This model is widely observed in cash-intensive jurisdictions.

4.3. Table: Combined Red Flags

Category	Indicator	Why It Matters
Financial	frequent small transfers from different senders	smurfing and concealment



Category	Indicator	Why It Matters
Cash	same-day withdrawals	suggests immediate operational use
Travel	unexplainable travel after receiving funds	logistical support
Digital	presence of crypto wallet apps	conversion and hiding of funds
NPO sector	donations without beneficiary lists	misuse of humanitarian narrative
Assets	sudden sale of property before travel	financing outbound movement
Network	third parties withdrawing cash	intermediaries reduce exposure

4.4. Diagram: Network Mapping – Core Nodes

Subject A

↑ financial flows

Intermediary B

↑ communication links

Donor C

↑ travel events

Organisation D

Combining these three streams (money + communication + movement) provides strong evidence of awareness and intent.

5. OPERATIONAL TECHNIQUES

5.1. “Follow-the-Money Plus” Method

An effective investigation must integrate:

1. financial flows
2. communication patterns
3. travel and logistical movement.

When these three lines intersect within the same time, evidentiary value increases significantly.

5.2. Role of Intermediaries



Intermediaries always display:

- low personal financial activity
- high cash withdrawal activity
- little or no declared income

They are the primary entry points for dismantling the network.

5.3. Lifestyle Analysis

Compare:

- declared income.
- actual expenses
- travel frequency
- app-based spending
- purchase of digital assets

Discrepancies are evidence of concealed activity.

5.4. Rapid Contradiction Test

A simple interview tool:

If the individual cannot explain:

- who the donor is.
- why did the donor choose them?
- what they did immediately after receiving funds
- why travel occurred

it strongly suggests awareness and intentional behaviour.

6. QUICK MODELS FOR IMMEDIATE USE

6.1. Quick Risk Model (1-Minute)

Each item = 1 point

Score of 4 or above = high risk

- small frequent transfers
- intermediaries involved
- unknown donors



- same-day cash withdrawals
- unexplained travel
- asset sale before travel
- online humanitarian campaigns without evidence
- presence of crypto wallets

6.2. “Core Evidence Pack”

The investigator must collect:

1. financial flow timeline
2. communication timeline
3. travel timeline
4. KYC and digital traces
5. donor financial profile



Appendix 2

Detecting Terrorist Financing These are **detection indicators** for FIUs and financial institutions. This appendix identifies practical red flags (transactional patterns, account behaviour and customer indicators) that could amount to terrorist financing.

Customer Profile and Behaviour

- Inconsistent or vague information provided during onboarding.
- Refusal to provide source of funds or occupation.
- Use of aliases or multiple identities.
- Frequent travel to high-risk jurisdictions without clear business or personal rationale.
- Association with known extremists or individuals under investigation.

Account Activity

- Transactions inconsistent with the customer's known profile or business.
- Sudden activity in dormant or low-use accounts.
- Use of multiple accounts to move small amounts below reporting thresholds (structuring).
- Frequent cash deposits or withdrawals without business justification.
- Round-number transactions or repeated patterns lacking economic rationale.

Transaction Patterns

- Transfers to/from high-risk jurisdictions or conflict zones.
- Use of third-party accounts or intermediaries without clear links.
- Rapid movement of funds through multiple accounts or institutions.
- Use of informal value transfer systems (e.g., hawala) or unregulated remittance services.
- Donations to charities or non-profits that lack transparency or oversight.

Non-Profit and Business Entities

- Non-profit organizations with unclear or inconsistent stated objectives.
- Charities receiving large donations followed by rapid disbursements abroad.
- Businesses with minimal physical presence or operations inconsistent with financial activity.
- Use of shell companies or trusts to obscure ownership or control.
- Entities registered in secrecy jurisdictions or with nominee directors.

Technology and Payment Methods

- Use of prepaid cards, virtual currencies, or anonymous payment platforms.
- Multiple cash machine withdrawals in different regions or countries.
- Use of online banking to conduct cross-border transfers outside normal hours.



- Purchase of high-value items (e.g., gold, electronics) for resale or transport.
- Attempts to avoid detection by splitting transactions or using coded references.



Appendix 3

Investigative Framework for Terrorist Financing

1. Understand the Nature of Terrorist Financing

- Sources: Can be legal (e.g. donations, charities, business profits) or illegal (e.g. drug trafficking, extortion, kidnapping)
- Methods: Use of informal value transfer systems (e.g. hawala), cash couriers, trade-based laundering, and abuse of non-profit organizations
- Purpose: Funds may support recruitment, propaganda, logistics, or direct attacks.

2. Initiate Financial Investigations Early

- Treat financial investigation as a parallel track to terrorism investigations—not a secondary effort FATF.
- Use Suspicious Activity Reports (SARs) and financial intelligence from reporting entities.

3. Leverage Legal Powers and Tools

- Apply terrorism legislation to compel information sharing and enhance investigative reach.
- Request additional data from SARs.
- Use Account Freezing Orders and Civil Recovery powers under relevant laws.
- Utilize international instruments like the International Convention for the Suppression of the Financing of Terrorism (1999) to support cross-border cooperation.

4. Engage with the Reporting Entities

- Encourage proactive reporting and information sharing from banks, money service businesses, and charities.
- Provide typology briefings to help institutions recognize terrorist financing indicators.

5. Conduct Parallel Financial Profiling

- Map out financial networks of suspects, including associates and facilitators.
- Use forensic accounting and data analytics to trace funds and identify patterns.



Appendix 4

Prosecution Strategy

1. Build Strong Evidentiary Foundations

- Combine financial records, wire transfers, SARs, and witness testimony.
- Use forensic evidence to link funds to terrorist acts or organizations.

2. Apply Specific Terrorism Financing Offenses

- Charge under terrorism financing statutes rather than general money laundering laws when possible
- Demonstrate intent or knowledge that funds supported terrorism—even if the amount is small or the act was not completed.

3. Coordinate with Prosecutors Early

- Involve prosecutors during the investigation phase to ensure admissibility and strategic framing of charges.
- Consider plea agreements or cooperation deals to dismantle broader networks.

4. International Cooperation

- Use mutual legal assistance treaties (MLATs) and Interpol channels to trace cross-border flows.
- Participate in joint task forces and intelligence-sharing platforms.

5. Training and Capacity Building

- Regularly train officers on terrorist financing typologies, legal frameworks, and financial tools.
- Use FATF's Operational Issues – Financial Investigations Guidance as a reference for integrating financial investigations into broader AML/CFT efforts FATF.



Appendix 5

LEAs should adopt a structured, secure, and collaborative approach to data sharing to effectively tackle terrorist financing. This includes robust inter-agency coordination and proactive public-private partnerships.

Best Practice Guide: Data Sharing to Combat Terrorist Financing

1. Establish Legal and Governance Frameworks

- Define lawful basis for sharing under national legislate.
- Use formal Information Sharing Agreements (ISAs) to clarify scope, purpose, data types, retention, and safeguards.
- Designate competent authorities for terrorism-related data access and processing.

2. Enable Secure Inter-Agency Collaboration

- Create joint task forces and centres to coordinate intelligence across police, FIUs, customs, and security services.
- Use interoperable platforms with audit trails and access controls.
- Share structured threat intelligence including typologies, financial flows, and operational leads.

3. Build Public-Private Partnerships (PPPs)

- Engage financial institutions through models like the Joint Money Laundering Intelligence Taskforce (JMLIT) and EFIPPP (Europol's European Financial and Economic Crime Centre)
- Share typologies, red flags, and case studies to improve private sector detection and reporting.
- Establish operational PPPs for real-time threat sharing, especially during active investigations.
- Use FATF's PPP guidance to balance data protection, technology use, and AML/CFT objectives FATF.

4. Implement Technical and Procedural Safeguards

- Apply data minimization and purpose limitation principles.
- Use encryption, role-based access, and secure transfer protocols.
- Maintain logs and audit trails for all data disclosures.
- Conduct regular reviews and risk assessments of sharing practices.

5. Promote Strategic Intelligence Sharing

- Share strategic assessments and emerging threats with private sector and international partners.



- Use anonymized or aggregated data where full disclosure is not feasible.
- Coordinate with regulators and oversight bodies to ensure compliance and trust.

6. Address Gaps and Challenges

- Identify legal and operational barriers to cross-sector sharing.
- Develop common data standards and formats to improve interoperability.
- Invest in training and capacity building for both public and private stakeholders.



Appendix 5: Recommendations to Strengthen Targeted Financial Sanctions Implementation

This appendix outlines actionable measures for enhancing the effectiveness, coordination, and enforcement of TFS in line with FATF Recommendation 6 and 7.

1. Legal and Institutional Framework

- Establish clear and direct legal authority for asset freezing, designation, and enforcement of sanctions
- Designate a central competent authority to coordinate TFS implementation and ensure timely updates of sanctions lists
- Ensure sanctions lists are publicly accessible and promptly transposed from UN and other relevant bodies

2. Risk-Based Supervision and Compliance

- Conduct sectoral risk assessments to identify exposure to sanctions evasion, especially in high-risk sectors
- Issue detailed guidance to reporting entities on screening obligations, red flags, and reporting procedures
- Promote adoption of automated screening systems and internal controls across

3. Inter-Agency Coordination and Intelligence Sharing

- Strengthen coordination between FIUs, LEAs, customs, and supervisory bodies
- Facilitate public-private partnerships to share typologies, intelligence, and compliance challenges (see Appendix 4)
- Engage in cross-border cooperation

4. Monitoring, Enforcement and Evaluation

- Implement regular supervisory inspections and audits of TFS compliance programs
- Enforce penalties for breaches
- Develop performance indicators and evaluation frameworks to assess the impact and effectiveness of TFS measures



Reference List

- Alldridge P. (2003) Money laundering law: Forfeiture, confiscation, civil recovery, criminal laundering and taxation of the proceeds of crime (Bloomsbury).
- Basra, R. and Neumann, P. R. 'Criminal pasts, terrorist futures: European jihadists and the new crime-terror nexus' (2016) *Perspectives on Terrorism*, 10(6), 25-40.
- Bauer, K., & Levitt, M. (2020). Funding in Place: Local Financing Trends Behind Today's Global Terrorist Threat. International Centre for Counterterrorism (ICCT).
- BBC News (2014) 'Lee Rigby murder: Adebolajo and Adebawale jailed', 26 February 2014, available from <http://www.bbc.co.uk/news/uk-26357007>, accessed August 10, 2024.
- BBC News (2017) 'London attack: Who was Khalid Masood?', 26 March 2017, available from London attack: Who was Khalid Masood? - BBC News, <https://www.bbc.com/news/uk-39373766>.
- [BiH - United States Department of State](#)
- Brisard, J. and Martinez, D. 'Islamic State: The economy-based terrorist funding' (2014) Thomson Reuters 3.
- Cassella, S. 'Reverse Money Laundering' (2003) *Journal of Money Laundering Control* 7 92
- Cheney, E. A. (2005). Leaving no loopholes for terrorist financing: The implementation of the USA Patriot Act in the real estate field. *Vand. L. Rev.*, 58, 1705.
- CNN (2015) 'A timeline of the Charlie Hebdo terror attack', 10 January 2015, available from <http://edition.cnn.com/2015/01/08/europe/charlie-hebdo-attack-timeline/>, accessed August 10 2015.
- Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Anti-money laundering and counter-terrorist financing measures: BiH, Fifth Round Mutual Evaluation Report (MONEYVAL (2024)29, Council of Europe, December 2024.
- Coonan, T. and Thompson, R. 'Ancient Evil, Modern Face: The Fighting against Human Trafficking' (2005) *Georgetown Journal of International Affairs*, 6, 43-52.
- Council Common Position 2001/931/CFSP of 27 December 2001 on the application of specific measures to combat terrorism, [2001] OJ L 344/93.
- Council Regulation (2001) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, OJ L 344, 28.12.2001, 70–75.
- Counter Extremism Project (n/d), 'Bosnia & Herzegovina: Extremism and Terrorism' (Counter Extremism Project, undated) para 3 <https://www.counterextremism.com/countries/bosnia-herzegovina-extremism-and-terrorism>, accessed 10 November 2025.
- Crimm, N. J. (2003). High Alert: The Government's War on the Financing of Terrorism and Its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy. *Wm. & Mary L. Rev.*, 45, 1341.
- Europol (2025), European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT 2025) (24 June 2025) <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat>, accessed 10 November 2025.



- Ferwerda, J (2014) 'Definitions of money laundering in practice' in (eds) Unger, B., Ferweda, J., van den Broek, M. and Deleanu, I. *The Economic and Legal Effectiveness of the European Union's Anti-Money Laundering Policy* (Edward Elgar).
- Financial Action Task Force (2001) *FATF IX Special Recommendations* (Financial Action Task Force: Paris, 2001).
- Financial Action Task Force (2004) *FATF 40 Recommendations* (Financial Action Task Force: Paris, 2004).
- Financial Action Task Force (2011) *Organised Maritime Piracy and Related Kidnapping for Ransom*. (Financial Action Task Force: 2011).
- Financial Action Task Force (2012) 'FATF steps up the fight against money laundering and terrorist financing', February 16, 2012, available from <http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html>, accessed 19 September 2014.
- Financial Action Task Force (2012) 'Operational Issues - Financial investigations Guidance', June 2012, available from https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.coredownload.pdf, accessed 30 November 2025.
- Financial Action Task Force (2013) *The role of Hawala and other similar service providers in money laundering and terrorist financing* (Financial Action Task Force: 2013).
- Financial Action Task Force (2015a) 'FATF Report: Emerging Terrorist Financing Risk' (Paris, October 2015).
- Financial Action Task Force (2015b), *Best Practices on Combating the Abuse of Non-Profit Organisations* (Recommendation 8) (16 November 2023), <https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html>, accessed 10 November 2025.
- Financial Action Task Force (2021), 'Ethnically or Racially Motivated Terrorism Financing' (FATF, June 2021) <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html>, accessed 10 November 2025.
- Financial Action Task Force (2025a), *The FATF Recommendations* https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf, accessed 10 November 2025.
- Financial Action Task Force (2025b), *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems* (2022, as amended), <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html>, accessed 10 November 2025.
- Financial Action Task Force (2025c), *Comprehensive Update on Terrorist Financing Risks* (Paris, 8 July 2025), <https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html>, accessed 10 November 2025.
- Financial Action Task Force (FATF), *Guidance on Criminalising Terrorist Financing* (Recommendation 5) (October 2016), <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Criminalising-terrorist-financing.html>, accessed 10 November 2025.
- Freeman and Rueshen (2011). Freeman, M., & Ruehsen, M. (2013). *Terrorism financing methods: An overview. Perspectives on terrorism*, 7(4), 5-26.



- Gilmour, N. (2016). Understanding the practices behind money laundering—A rational choice interpretation. *International Journal of Law, Crime and Justice*, 44, 1-13.
- Gordon, R. (2011). Terrorism financing indicators for financial institutions in the United States. *Case W. Res. J. Int'l L.*, 44, 765.
- Hardouin, P. (2009). Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing. *Journal of financial crime*, 16(3), 199-209.
- HM Government House of Commons Report of the Official Account of the Bombings in London on 7th July 2005 (House of Commons: London, 2005).
- HM Treasury and Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2025 (2025), https://assets.publishing.service.gov.uk/media/6877be59760bf6cedaf5bd4f/National_Risk_Assessment_of_Money_Laundering_and_Terrorist_Financing_2025_FINAL.pdf, accessed 10 November 2025.
- International Convention for the Suppression of the Financing of Terrorism, 9 December 1999, 2178, UNTS 197.
- Kenny, C., and Malik, N. 'Trafficking terror and sexual violence: Accountability for human trafficking and sexual and gender-based violence by terrorist groups under the Rome Statute' (2019) *Vanderbilt Journal of Transnational Law* 52, 43.
- National Commission on Terrorist Attacks Upon the United States (2004) *The 9/11 Commission Report: final Report of the National Commission on Terrorist Attacks Upon the United States* (National Commission on Terrorist Attacks Upon: Washington DC,). Baradaran, S., Findley, M., Nielson, D., & Sahrman, J. (2013). Funding terror. *U. Pa. L. Rev.*, 162, 477.
- Nepoleoni, L. 'Terrorism Financing in Europe' in Trinkunas, H. and Giraldo, J. (eds) *Terrorism Financing and State Responses* (Stanford University Press: 2007).
- Official Journal of the European Communities (2001), L 344/93.
- Royal United Services Institute (2025) *Reassessing the Financing of Terrorism in 2025* (Insights Paper, 11 September 2025), <https://www.rusi.org/explore-our-research/publications/insights-papers/reassessing-financing-terrorism-2025>, accessed 10 November 2025.
- Ryder N (2024) 'To report or not to report? An analysis of the relationship between defence against terrorism financing suspicious activity reports and fraud in the United Kingdom' In de Koker, L and Goldbarsht, D *Financial Crime, Law and Governance – Navigating Challenges in Different Contexts* (Springer) 169-202.
- Ryder, N (2025) 'Coordinated terrorist financing – an emerging threat or a glaring omission? Time to rethink the Financial War on Terrorism' In (eds) de Koker, L and Goldbarsht, D., de Koker L and Ferrill, J *Combating Financial Crime: intended and unintended consequences* (Springer) accepted for publication.
- Ryder, N. 'Out with the old and ... in with the old? A critical review of the Financial War on Terrorism on the Islamic State of Iraq and Levant' (2018b) *Studies in Conflict and Terrorism*, 41(2), 79-95.
- Ryder, N., Bourton, S., Hall, D. and Hillman, H. 'Higher Education Institutions and the Anti-Money Laundering and Counter-Terrorism Financing Regulations' (2023) *Criminal Law Review*, 9, 560-580.



- Samantha Maitland Irwin, A., Raymond Choo, K. K., & Liu, L. (2011). An analysis of money laundering and terrorism financing typologies. *Journal of Money Laundering Control*, 15(1), 85-111.
- Sinaee, V. and Khatibi, A. 'Taliban political economy (2001-1996)' (2023) *Central Eurasia Studies*, 16(1), 223-248.
- United Nations (n/d) 'Chapter VII: Action with respect to threats to the peace, breaches of the peace, and acts of aggression', n/d, available from <http://www.un.org/en/documents/charter/chapter7.shtml>, accessed 31 October 2025.
- United Nations Security Council (2001a), 'Resolution 1368 (2001)' S/RES/1368 (12 September 2001) <https://digitallibrary.un.org/record/448051>, accessed 10 November 2025.
- United Nations Security Council (2001b), 'Resolution 1373 (2001)' S/RES/1373 (28 September 2001) <https://digitallibrary.un.org/record/449020>, accessed 10 November 2025.
- United States Department of Treasury National Terrorist Financing Risk Assessment 2015 (United States Department of Treasury: 2015).
- Van de Bunt, H. (2008). The role of hawala bankers in the transfer of proceeds from organised crime. *Organized crime: Culture, markets and policies*, 113-126.
- Wagman, Shlomit. 'Cryptocurrencies and national security: the case of money laundering and terrorism financing' (2022) *Harvard National Security Journal*, 14, 87-101.
- Williams, P. 'Terrorist financing and organized crime: nexus, appropriation, or transformation?' In Bierskeker, T. and Eckert, S. (eds) *Countering the financing of terrorism* (Routledge: 2007) pp. 142-165.

