FATF

FATF REPORT

Comprehensive Update on Terrorist Financing Risks

July 2025

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit www.fatf-gafi.org.

This report was produced with contributions from across the FATF's Global Network, including from France and the UN Security Council Counter-Terrorism Committee Executive Directorate as project co-leads.

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE (CTED)

Legal information:

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Terrorist organisations referred to in this report have either been designated by the United Nations Security Council (UNSC) pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida (AQ) and associated individuals, groups, undertakings and entities, or through regional and national designation regimes developed pursuant to UNSC resolutions 1373 (2001) and 2462 (2019) for the purposes of asset freezing. As such, mentioning of an organisation in the analysis or case studies included in this report does not entail or imply the endorsement of any national or regional designations by the United Nations (UN). Moreover, jurisdictions remain sovereign in their determination as to whether to incorporate regional or other national asset-freezing lists domestically, should they meet their own designation criteria, and pursuant to their own legal and regulatory frameworks. References made in the report based on regional or national designations regimes, do not entail or imply the endorsement of any national or regional designations by any other jurisdictions.

Citing reference:

FATF (2025), *Comprehensive Update on Terrorist Financing Risks*
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html

© 2025 FATF/OECD. All rights reserved.
No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org)

Photocredit coverphoto: Jacek Wojnarowski/Shutterstock.com

Table of Contents

© FATF-OECD 2025

© FATF-OECD 2025

© FATF-OECD 2025

Acronyms

Acronym	Description
AI	Artificial intelligence
AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
ATM	Automated teller machine
CDD	Customer due diligence
CFT	Countering the financing of terrorism
DNFBP	Designated non-financial businesses and professions
DRC	Democratic Republic of Congo
EAG	Eurasian Group on Combating Money Laundering and Financing of Terrorism
EPOM	E-commerce platform
EoRMT	Ethnically or racially motivated terrorism
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FSRB	FATF-Style Regional Body
FTF	Foreign terrorist fighter
FTZ	Free trade zone
FI	Financial institution
GABAC	Action Group Against Money Laundering in Central Africa
GAFILAT	Financial Action Task Force of Latin America
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
HOSSP	Hawala and other similar service providers
IAT	Illicit arms trade
IBAN	International bank account number
INTERPOL	International Criminal Police Organisation
KFR	Kidnapping for ransom
KYC	Know Your Customer
LEA	Law enforcement authority
MENAFATF	Middle East and North Africa Financial Action Task Force
MER	Mutual Evaluation Report
MSB	Money service business
MVTS	Money value transfer service
NPO	**Non-profit organisation**
NRA	National risk assessment
P2P	Peer-to-peer
PPP	Public-private partnership
PSP	Payment service provider
RUSI	Royal United Services Institute
SALWs	Small arms and lights weapons
SGBV	Sexual and gender-based violence
SNS	Social networking service
TBML	Trade-based money laundering
TBTF	Trade-based terrorist financing
TF	Terrorist financing
TPC	Targeted public consultation
UN	United Nations
UN CTED	UN Counter-Terrorism Committee Executive Directorate
UNESCO	UN Education, Scientific and Cultural Organisation
UNICRI	UN Interregional Crime and Justice Research Institute
UNODC	UN Office of Drugs and Crime

© FATF-OECD 2025

UNSC	UN Security Council
UNSCR	UN Security Council Resolution
VA	Virtual asset
VASP	Virtual asset service provider
WCO	World Customs Organisation

Listing reference of entities subject to measures imposed by the UNSC Committee pursuant to resolutions 1267, 1989 and 2253 concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities.

Acronym	Description	Listing references
Al Furqan	Al Furqan	QDe.107
Al Rashid Trust	Al-Rashid Trust	QDe.005
ANF (a.k.a. HTS)	Al-Nusrah Front for the People of the Levant, also known as Hay'at Tahrir al-Sham (HTS)	QDe.137
Ansar al-Islam	Ansar al-Islam	QDe.098
AQ	Al-Qaida	QDe.004
AQAP	Al-Qaida in the Arabic Peninsula	QDe.129
AQIM	The Organization of Al-Qaida in the Islamic Maghreb	QDe.014
ASG	Abu Sayyaf Group	QDe.001
Boko Haram	Jama'atu Ahlis Sunna Lidda'Awati Wal-Jihad, also known as Boko Haram	QDe.138
ISGS	Islamic State in the Greater Sahara	QDe.163
ISIL	Islamic State of Iraq and the Levant (listed as Al-Qaida in Iraq)	QDe.115
ISIL-K	Islamic State of Iraq and the Levant – Khorasan	QDe.161
ISIL-SEA	Islamic State of Iraq and the Levant in South-East Asia	QDe.169
ISWAP	Islamic State West Africa Province	QDe.162
JiM	Jaish-I-Mohammed	QDe.019
JNIM	Jama'a Nusrat ul-Islam wa al-Muslimin	QDe.159
LeT	Lashkar-E-Tayyiba	QDe.118
TTP	Tehrik-e-Taliban Pakistan	QDe.132

© FATF-OECD 2025

Executive summary

1. Since the release of its last comprehensive update on terrorist financing (TF) risks in 2015, countering the financing of terrorism (CFT) has remained a strategic priority for the Financial Action Task Force (FATF). Over the past decade, terrorists have demonstrated a persistent ability to exploit the international financial system to support their activities and carry out attacks. While the methods they employ can vary widely, the overall trend underscores their adaptability and determination. This continued abuse of the financial system poses a serious threat to global security and undermines international peace.

2. In this context, the 4th Round of Mutual Evaluations, conducted across over 194 jurisdictions in collaboration with the nine FATF-Style Regional Bodies (FSRBs), revealed that 69% of assessed jurisdictions exhibited major or structural deficiencies in effectively investigating, prosecuting, and convicting terrorism financing cases. Such deficiencies have also recently been highlighted by UN CTED[1].

3. These findings highlight the need for jurisdictions to maintain an evidence-based understanding of TF risks, avoiding assumptions that could lead to ineffective, disproportionate measures and potential breaches of international law, including human rights obligations.

4. Therefore, this report aims to support jurisdictions by:

- Enhancing the understanding of TF risks among competent authorities, the private sector, non-profit organisations (NPOs), academia, and other stakeholders, offering an up-to-date overview of the factors shaping TF risks in 2025 and examining how terrorist groups raise, move, store, and use funds, with a focus on evolving financial management structures.
- Identifying emerging trends to help jurisdictions anticipate possible evolution of the TF risks in the near future.
- Strengthening jurisdictions' capacity to respond by refining risk assessment methodologies, developing risk-based regulatory frameworks, enhancing enforcement, and tailoring CFT strategies. This includes updating risk indicators to reflect national contexts and directing resources towards areas of highest risk, thereby improving detection, prevention, and response capabilities.
- Equipping the private sector and civil society actors with insights to support more effective risk management and compliance and encouraging academia to build upon this research to deepen the understanding of TF dynamics and contribute to the development of innovative approaches to counter TF.

5. This report builds on the FATF's 2015 report on Emerging Terrorist Financing Risks as well as all relevant typologies, indicators and guidance published by the FATF over the past decade. It also consolidates many TF-related sectorial and thematic reports issued since 2015.

[1] UN CTED, Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions - with a focus on investigating and prosecuting the financing of terrorism, December 2023, available at Thematic summary assessment of gaps- investigating and prosecuting the financing of terrorism (2023).

© FATF-OECD 2025

6. Terrorist organisations referred to in this report have either been designated by the United Nations Security Council (UNSC), or through regional and national designation regimes developed pursuant to UNSC resolutions 1373 (2001) and 2462 (2019) for the purposes of asset freezing.

7. To assess the evolving TF risk landscape, the project team, comprising experts from 18 FATF members, 4 FSRB Secretariats, 8 FSRB members, and 3 FATF Observers, co-led by experts from France and the UN CTED, with support from the FATF Secretariat, conducted the following:

- Reviewed open-source materials, including FATF 4th Round Mutual Evaluation reports, FATF publications, FSRB reports, and national risk assessments from FATF and FSRB jurisdictions.
- Analysed responses from 82 delegations to two project questionnaires, including case studies and TF risk indicators.
- Evaluated input from 842 entities across academia, civil society, think tanks, and the private sector through a targeted public consultation.
- Collected oral and written feedback during the FATF Joint Experts' Meeting in January 2025.

8. The report is structured in four sections, supplemented by an annex listing TF risk indicators derived from data provided by delegations in response to the project's questionnaires and from previous FATF reports.

9. The first section of the report outlines a non-exhaustive set of factors that influence the nature of TF risks. These include materiality factors, the types of terrorist actors involved, and other considerations. Depending on contextual circumstances, terrorist organisations and individuals exhibit varying financial needs and consequently adapt their financial management strategies accordingly. Terrorist actors of a similar type may adopt different financing methods depending on the situation, and comparable factors can affect them in divergent ways.

10. Material factors that can create financing opportunities for terrorist organisations include territorial control; proximity to, or involvement in, armed conflict; access to, or control over, natural resources, weak governance and high levels of corruption; border vulnerabilities; the prevalence of informal or cash-based economies; State sponsorship; and the existence of free trade zones.

11. TF tactics also vary significantly depending on the type of actor involved. Networked terrorist organisations often rely on regional and domestic affiliates and receive substantial global donations, increasingly using decentralised regional hubs to manage complex, cross-border financial networks. In contrast, non-affiliated regional and domestic groups operate independently within specific areas and tend to rely on local resources. Ethnically or racially motivated actors, who are not always formally designated as terrorists, have more options to raise funds through lawful and overt means. Small unaffiliated terrorist cells and individual terrorists—including foreign terrorist fighters (FTFs)—typically have minimal financial needs and require little external support.

12. Other factors influencing TF tactics include exposure to terrorist propaganda, the varying internal financial management structures of terrorist organisations—ranging from highly centralised to increasingly decentralised models. Readers are also encouraged to take into consideration gender when analysing TF risks and working on CFT policies.

© FATF-OECD 2025

13. Section 2 of the report provides an overview of current methods employed by terrorist organisations and individuals to raise, move, store, and use funds and assets, highlighting the growing interconnections between these channels. Informal mechanisms such as cash transportation and hawala and other similar service providers (HOSSPs) remain widely used, particularly in conflict zones and remote areas with limited financial infrastructure, offering anonymity and operating outside regulated systems. These methods continue to evolve, with large terrorist networks adopting digital adaptations of HOSSPs, including blockchain-based pseudo-anonymous transfers.

14. Similarly, the report underscores the growing popularity of online payment services and mobile money platforms, which are particularly attractive in jurisdictions with lax regulation.

15. Despite improvements in transparency and identity verification, terrorists continue to make use of formal financial services, including deposit accounts, wire transfers, and prepaid cards.

16. Digital platforms—such as social media, messaging applications, and crowdfunding sites—are increasingly abused for TF, particularly when they offer integrated payment services that bypass due diligence. Although the level of abuse of virtual assets (VAs) by terrorists remains difficult to measure precisely, their use is increasing, with some groups systematically leveraging VAs and employing obfuscation techniques and/or shifting towards alternatives VAs promoted as more private and secure.

17. Moreover, the misuse of legal entities—including shell companies, trusts, and NPOs—remains a persistent concern. These structures are used to transfer or launder funds and to support terrorist operations, with some terrorist organisations leveraging sham NPOs or abusing legitimate ones for fundraising, recruitment, and logistical support and/or operating legitimate cash-intensive businesses to generate revenue for TF in their areas of control.

18. To generate revenue, terrorist organisations have also been reported to exploit, trade and trafficking natural resources (energy commodities, agricultural products, wildlife, precious metals and stones, etc). They are also relying, sometimes to a large extent, on proceeds from various criminal activities: extorsion, kidnapping for ransom, human trafficking and trafficking and smuggling of goods, including drugs and arms, etc.

19. Section 3 of the report outlines key trends in the evolution of TF over the past decade. While traditional financing channels and schemes continue to be used, there is a marked increase in the interlinkage of diverse methods and the integration of digital technologies with conventional techniques, adding new layers of complexity to TF activities. Operations have become increasingly decentralised, with regional financial hubs and self-financed cells playing a larger role, adapting to local contexts, and employing a broader range of funding sources, from criminal proceeds to investments in business activities.

20. In parallel, the threat posed by lone individuals—often younger in age—is rising, with such actors relying on microfinancing strategies drawn from both licit sources (e.g., salaries, social benefits, family support), petty criminal activity, as well as technology-enabled methods, including gaming and social media features. These microfinancing methods are especially difficult to detect due to their mundane financial footprints.

21. Geographically, the report notes that sub-Saharan Africa—particularly the Sahel — has emerged as the global epicentre of terrorism, significantly influencing the patterns and geography of TF flows. Developments in Syria and their potential impact on TF-related

© FATF-OECD 2025

financial flows also requires close and continuous monitoring. ISIL-Khorasan continues to pose a significant threat in Afghanistan but also in Europe and Central Asia, where it actively seeks to recruit and fundraise relying on advances propaganda tactics to gather support.

22. Looking ahead, the report lays out several anticipated challenges. With multiplying armed conflicts that also involve terrorist activity and continuing exploitation of humanitarian causes for terrorist propaganda, the risk of humanitarian aid being diverted for TF should be monitored, while ensuring full respect for international humanitarian law. In addition, resource scarcity, especially food insecurity driven by conflict and climate-related events, may also heighten regional vulnerability to exploitation by terrorist actors through looting and coercion. Finally, the enduring convergence between organised crime and TF is likely to reinforce the use of cash as a preferred channel.

23. Section 4 outlines key recommendations, including:

- Addressing the transnational dimension of TF risks through coordinated, multilateral responses. The global nature of TF necessitates concerted international action. This involves making the multilateral designation of terrorist organisations under UNSC sanctions regimes a primary priority, alongside regional and national mechanisms established pursuant to UNSCR 1373.
- Strengthening the implementation of FATF Standards. Effective application of the FATF Standards—particularly in high-risk areas such as MVTS, virtual asset service providers (VASPs), and legal persons—is essential to harmonise legal frameworks and reduce the ability of terrorist organisations to exploit regulatory gaps and inconsistencies.
- Expanding outreach to uncovered sectors. As terrorist groups and individuals increasingly avoid traditional financial systems, it is crucial to engage sectors not currently covered by the FATF Standards, such as social media and messaging platforms. This may entail developing targeted public-private partnerships to better understand and address emerging threats.
- Incorporating CFT considerations into broader technical assistance cooperation. The FATF community should ensure that wider capacity-building and technical assistance initiatives integrate CFT priorities and leverage the FATF Standards to establish effective and sustainable frameworks. This includes exploring how FATF can mobilise its own expertise—and that of the Global Network—to support relevant technical assistance programmes by incorporating a dedicated CFT dimension.
- Enhancing FATF support for private sector CFT efforts. Additional measures should be considered to strengthen FATF's support for the private sector, such as creating a centralised online repository of relevant materials, developing targeted communication strategies, and providing awareness-raising and training activities through both in-person and online formats.
- Safeguarding humanitarian activity. CFT measures must consider their potential impact on humanitarian operations, ensuring that measures do not impede activities conducted in accordance with international humanitarian law by impartial humanitarian actors.

© FATF-OECD 2025

24. The report concludes with a call to further strengthen risk analysis, recognising that new TF schemes may continue to emerge or come to light. Enhancing our collective understanding of TF risks will require sustained efforts through regularly updated national, supranational, sectoral, and emerging risk assessments in the years ahead.

© FATF-OECD 2025

Introduction

Purpose, scope and objectives.

25. Countering the financing of terrorism (CFT) continues to be a priority[2] for the Financial Action Task Force (FATF), given the serious ongoing and evolving threats posed by terrorists around the world. These threats range from small cells or lone individuals to large-networked terrorist organisations operating across borders and/or possessing territorial control capabilities.

26. For the past decade, terrorists have demonstrated their persistent ability to abuse the international financial system to support their activities and carry out attacks, ultimately undermining international peace and security. The ways in which financing methods are used by terrorist actors can vary considerably depending on the proximity and scope of the terrorism threat, availability of technologies, the terrorists' financial needs, and the regional and economic contexts. Therefore, understanding risks and trends in the financing of various terrorist organisations and individual terrorists is crucial to identify and dismantle their financial and economic networks, and disrupt the flow of funds sustaining their activities. Legal and enforcement responses that are based on assumed, rather than evidence-based, TF risks of are often ineffective, unnecessary, and disproportionate, and risk violating international law, including international human rights law[3].

27. In February 2024, the FATF agreed to conduct further research on the methods employed by individual terrorists, terrorist organisations, and violent extremists to finance their activities, depending on the context in which they operate. In doing so, this report will provide a comprehensive and up-to-date overview of the various methods they use to raise, move, store, and spend their funds and other assets, and how these mechanisms have evolved in the last decade.

28. Terrorist organisations referred to in this report have either been designated by the United Nations Security Council (UNSC) pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh)[4], Al-Qaida (AQ) and associated individuals, groups, undertakings and entities[5], or through regional and national designation regimes developed pursuant to UNSC resolutions 1373 (2001) and 2462

---

2 FATF Declaration of the Ministers, paragraph 9 "Considering the serious ongoing threat of terrorism in many regions of the world, the FATF will also continue its strategic focus on countering terrorist financing, including cross-border terrorist financing, and other emerging trends and providing our members and private sector partners with updated typologies and risk indicators. We commit to and encourage all jurisdictions to strengthen cooperation to better detect, investigate, prosecute and disrupt terrorist financiers", 18 April 2024 (www.fatf-gafi.org)

3 UNSC Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 17, available at S/2025/22 .

4 In this report, referenced as ISIL.

5 By resolution 2734 (2024), the Security Council imposes individual targeted sanctions (an assets freeze, travel ban, and arms embargo) upon individuals, groups, undertakings and entities designated on the ISIL (Da'esh) & Al-Qaida Sanctions List: UNSC 1267 AQ Sanctions List (www.un.org).
The UNSC Consolidated List includes all individuals and entities subject to measures imposed by the Security Council. The inclusion of all names on one Consolidated List is to facilitate the implementation of the measures, and neither implies that all names are listed under one regime, nor that the criteria for listing specific names are the same.

© FATF-OECD 2025

(2019) for the purposes of asset freezing. As such, mentioning of an organisation in the analysis or case studies included in this report does not entail or imply the endorsement of any national or regional designations by the United Nations (UN). Moreover, jurisdictions remain sovereign in their determination as to whether to incorporate regional or other national asset-freezing lists domestically, should they meet their own designation criteria, and pursuant to their own legal and regulatory frameworks[6]. References made in the report based on regional or national designations regimes, do not entail or imply the endorsement of any national or regional designations by any other jurisdictions[7].

29. The report organises the analysis into different sections:

- Section 1: Factors influencing the nature of TF risks.
- Section 2: Methods used to raise, move and manage funds and other assets for TF purposes.
- Section 3: Terrorist financing risks evolution and anticipated trends.
- Section 4: Recommendations.
- Annex A: TF risk indicators.

30. This report aims to help competent authorities from the FATF Global Network, the private sector, non-profit organisations (NPOs) and other relevant stakeholders better understand the nature of global and context-specific risks and trends related to TF, and more efficiently mitigate TF risks based on a risk-based implementation of FATF Standards. In addition, it will contribute to the revision and update of TF risks indicators applicable to each context. By offering a more granular understanding of the way in which terrorists exploit jurisdictional vulnerabilities for financing purposes, this report will also provide an analysis on the evolution of these trends and an assessment of the anticipated risks over the next three to five years.

Methodology, participants and data utilised

31. Experts from France and the United Nations Counter-Terrorism Committee Executive Directorate (UN CTED) co-lead the project team with support from the FATF Secretariat. The Project Team consisted of experts drawn from 18 FATF members[8], 4 FATF-style Regional Bodies (FSRBs) Secretariats[9], 8 FSRBs members[10], and 3 FATF Observers[11].

32. This paper builds on the FATF 2015 report on Emerging Terrorist Financing Risks[12], the last report to be published with a comprehensive approach to TF, including all

6 See, UN Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism, "Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions", S/2019/998, December 2019, paragraph 56—available at S/2019/998

7 Please refer to the jurisdictions' respective national designations list.

8 Australia, Canada, Denmark, European Commission, India, Indonesia, Italy, Israel, Germany, Luxembourg, Malaysia, Mexico, Türkiye, Singapore, South Africa, Spain, United States, and United Kingdom.

9 APG, GIABA, EAG and ESAAMLG Secretariats.

10 Bahrein, Burundi, Cayman Islands, DRC, Dominican Republic, Ecuador, Malawi, and Malta.

11 UN (UN CTED, UNOCT, 1267 Monitoring Team), UNODC and OSCE.

12 FATF Emerging Terrorist Financing Risks, October 2015

© FATF-OECD 2025

relevant typologies, indicators and guidance published by the FATF over the past decade. It also consolidates many TF-related sectorial and thematic reports issued since 2015.[13]

33. The report findings are based on:

- A review of the existing open-source materials on this topic, including the FATF Global Network 4th Round Mutual Evaluation reports (MERs)[14], FATF publications[15], reports and analytical materials produced by FSRBs Secretariats and other international and regional organisations (including FATF Observers). It also included an extensive analysis of publicly available national risk assessments (NRAs) conducted by FATF and FSRB jurisdictions.
- Responses to the two project questionnaires sent to the FATF Global Network: 82 delegations[16] provided information on a variety of topics including case studies and risk indicators for TF activities.
- Answers received to the targeted public consultation (TPC) process: 842 entities from academia, civil society, think tanks, and the private sector

[13] *E.g.,* FATF Risk of terrorist abuse in non-profit organisations (2014), Financing of Recruitment for Terrorist Purposes (2018), Ethnically or Racially Motivated Terrorism Financing(2021), Misuse of Citizenship and Residency by Investment Programmes (2023), Money Laundering and Terrorist Financing in the Art and Antiquities Market (2023), Crowdfunding for Terrorism Financing (2023)

[14] Based on the Secretariat's analysis of 185 published MERs (available in www.fatf-gafi.org). While efforts were made to ensure comprehensive coverage, variations in terminology across MERs mean that some relevant references may not have been captured by the search terms used. As a result, there may be some omissions in the dataset. Nonetheless, the Secretariat considers the dataset sufficiently accurate and complete to support a robust and representative analysis.
To extract relevant data, the Secretariat employed a combination of carefully selected keywords and flexible regular expressions, designed to account for a wide range of punctuation styles and formats. This approach was applied consistently across all published MERs, using a regex-based search tool to identify and retrieve sentences, paragraphs, and sections referencing specific types of terrorist financing. While this method aimed to be as exhaustive as possible—capturing standard terminology and common variations—some margin of error is inherent in the process. This may be due to atypical formatting, unconventional punctuation, misspellings, or diverse vocabulary used across different MERs. As such, it is possible that not every single reference was identified.
Nonetheless, the frequency with which these topics appear in most MERs—often multiple times—greatly mitigates the risk of omission. Even if an isolated mention was missed, it is highly likely that the same theme or reference was captured elsewhere within the same report.

[15] Available at www.fatf-gafi.org

[16] Andorra, Angola, Armenia, Australia, Bahrain, Belgium, Botswana, Burundi, Canada, Cayman Islands, China, Denmark, Ecuador, El Salvador, Ethiopia, Europol, France, GABAC Secretariat, Germany, Greece, Guatemala, Honduras, India, Indonesia, INTERPOL, Iraq, Israel, Italy, Ivory Coast, Japan, Kenya, Korea, Kyrgyzstan, Lebanon, Luxembourg, Madagascar, Malaysia, Malta, Mauritius, MENAFATF Secretariat, Mexico, Moldova, Morocco, Mozambique, Namibia, Nauru, Netherlands, Nicaragua, North Macedonia, Pakistan, Palestinian Authority, Paraguay. Portugal, Qatar, Russian Federation*, Rwanda, Saudi Arabia, Senegal, Serbia, Seychelles, Singapore, Slovenia, South Africa, Spain, Sweden, Switzerland, Syria, Tajikistan, Tanzania, Thailand, Tunisia, Türkiye, Uganda, UN 1267 Monitoring Team, UN CTED, United Arab Emirates, United Kingdom, United States, Uzbekistan, Yemen, Zambia, and Zimbabwe. *The FATF Plenary suspended FATF membership of the Russian Federation on 24 February 2023 [FATF Statement on Russian Federation].

© FATF-OECD 2025

stakeholders provided information on their experience and views on TF methods and developed indicators.

- Oral feedback and additional material received from project team members and participants at the FATF Joint Experts' Meeting (Terrorist Financing Track)[17] to the preliminary draft report, and consecutive written feedback[18].

34. The report reader should note that the information provided by delegations through the project questionnaires, targeted public consultation and oral feedback received from project team members and participants at the JEM, has been analysed and embedded in the main draft report without providing references to the owner of the information in compliance with FATF data protection and privacy rules.

Terminology

35. The report uses the following key concepts from the FATF Terrorist Financing Risk Assessment Guidance[19]:

- A **TF risk** is a function of three factors: threat, vulnerability, and consequence. It involves the risk that funds or other assets intended for a particular terrorist or terrorist organisation are being raised, moved, stored, or used in or through jurisdiction, whether funds or other assets were legally or illegally acquired in the first place.

  a) A **TF threat** is a person or group of people[20] with the potential to cause harm by raising, moving, storing, or using funds or other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations.

  b) The concept of **vulnerability** comprises those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type or service that makes them attractive for TF. Vulnerabilities may also include weaknesses in measures designed specifically for CFT[21], or more broadly in AML/CFT systems or controls, or contextual features of a jurisdiction that may impact opportunities for terrorist financiers to raise or move funds or other assets (e.g., large informal economy, porous borders). There may be some overlap in the vulnerabilities exploited for both ML and TF.

  c) In the TF context**, consequence** refers to the impact or harm that TF threat may cause if eventuated. This includes the effect of the underlying terrorist activity on domestic or institutional financial systems and institutions, as

---

17 Hosted by UNODC at the Vienna International Centre, from 8-10 January.

18 Written feedback received from: APG Secretariat, Canada, El Salvador, European Commission, Germany, GIABA Secretariat, India, Indonesia, Israel, Luxembourg, Malta, MENAFATF Secretariat, Netherlands, Türkiye, United States, and UNODC.

19 Terrorist Financing Risk Assessment Guidance (2019).

20 This may include both natural and legal persons.

21 FATF Recommendation 5 (R.5) and Recommendation 6 (R.6) set out in detail the specific requirements to criminalise TF and implement targeted financial sanctions on the basis of the International Convention for the Suppression of the Financing of Terrorism (1999), and relevant UN Security Council Resolutions (UNSCRs).

© FATF-OECD 2025

well as the economy and society more generally. Notably, consequences of TF are likely to be more severe than for ML or other types of financial crime (e.g., tax fraud), which impacts how countries respond to identified threats. Consequences of TF are also likely to differ between countries and between TF channels or sources, and may relate to specific communities or populations, the business environment, or national interests.

36. In addition, this report utilises specific terminology from the FATF General Glossary[22] on the understanding of the different type of actors involved in TF activities:

- The term **terrorist act** includes:
  a) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).
  b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act.
- The term **terrorist** refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
- The term **terrorist organisation** refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons

22 FATF General Glossary (www.fatf-gafi.org)

© FATF-OECD 2025

acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

37. Therefore, **terrorist financing** is the financing of terrorist acts, and of individual terrorists and terrorist organisations.

© FATF-OECD 2025

Section 1: Factors influencing the nature of terrorist financing risks

38. From lone actors committing attacks requiring very low financial means to terrorist groups that have territorial control and benefit from large financial networks, each jurisdiction is exposed to specific TF risks according to the country's national or sub-national context, materiality, and structural elements. Depending on contextual factors, terrorist organisations and individual terrorists will have different financial needs and, as a result, will adapt their own financial management strategies to these factors. Additionally, varying factors related to socio-economic environments (e.g., economic stability, governance, crime levels), proximity to armed conflicts, access to natural resources, levels of convergence of their activities with legal businesses or criminal activities, as well as the levels of scrutiny and effectiveness of CFT measures, will impact the way terrorist groups and individuals attempt to raise, move, store, and spend funds and other assets. Understanding terrorists' financial tradecraft in context-specific circumstances is crucial to ascertain how, when, and why they adopt specific methods to finance their activities[23]. This insight will enable each jurisdiction to tailor its counter-terrorism policies and CFT national strategies, by focusing attention to where it is most exposed to risks, developing relevant tools and efficiently allocating resources.

39. The report offers a non-exhaustive analysis of factors that may influence nature of the TF risks faced in certain geographies at a certain point of time. Those factors are not mutually exclusive, and the specificities associated with them in the current section in terms of financing needs and methodology are indicative, as they can evolve quickly as situations change. At the same time, it is noteworthy that similar types of terrorist actors may act differently in terms of their financing methods in different types of situations, and comparable factors may affect them differently. References to specific terrorist groups of individuals are used as case-specific examples of observed contextual trends or financial behaviour patterns and are not meant to suggest that certain terrorist actors only operate with specific methods.

1. Materiality factors

1.1. *Territorial control*

40. Territorial control is one of the most significant factors influencing how terrorist organisations generate income, exploit sources of revenue, and manage their finances. Such control can take different forms and scale, from a State-like operation to a control over a restricted area. Areas, where infrastructures and government services lacking and legitimate institutions are unable to assert authority, are particularly exposed.

41. Territorial control within a country or a region enables various forms of extortion from local populations, and makes it possible to maintain large-scale financial networks through comprehensive taxation-like systems, including coerced road "taxes"; fees and "taxes" on commercial activities and proceeds from trade; "licensing" of excavation of resources or cultural property, and/or agricultural production; issuance of vehicle licence plates and registration; and customs duties, among others. In some cases, territorial control also grants terrorist organisations direct access to natural resources and allows

[23] See by analogy, United Nations Security Council Counter-Terrorism Committee, Non-binding principles for Member States on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes (S/2025/22), paragraph 17.

© FATF-OECD 2025

them to extort businesses in sectors such as agricultural or mining. Gaining control over a territory can also provide financial resources through spoils of war, such as raiding central bank reserves, accessing weapons stockpiles or looting cultural heritage sites.

42. In most cases, territorial control comes with larger-scale overt methods to raise, move, store, and spend funds and other assets, and aims to target groups of population or businesses within the controlled territory, sometimes under a pretext of protection or security. In such situations, terrorist financial flows occurring within the controlled area are unhindered and not subject to controls, since the financial and economic systems are part of the controlled area or territory. To transfer funds into or out of such areas, terrorists may exploit networks that misuse formal financial systems, often resorting to obfuscated methods. In some cases, the financial system within the controlled territory holds financial ties with other jurisdictions, thus allowing for the movement of funds.

43. Territorial control may also come with specific expenditures when a terrorist organisation aims at adopting administrative functions or delivering public services to the population within the area it controls. These may include, for example, the payment of salaries to fighters or the execution of infrastructure works.

44. Conversely, the loss of territorial control is also a determining factor to consider as it prompts terrorist organisations to turn towards more dispersed revenue streams, often relying on fundraising and online methods. It has also been reported that some of ISIL's physical cash reserves were buried in the ground in Iraq and the Syrian Arab Republic. Due to the relative scarcity of resources currently faced by the group, ISIL has excavated these cash reserves and smuggled funds out.

1.2. Proximity to, or involvement in, armed conflicts

45. According to the 2025 Global Terrorism Index[24], conflict has been the primary driver of terrorism since 2007, and 98% of terrorism-related deaths occurred from 2007 to 2024 in countries that were involved in a conflict at the time of the attacks. In 2024, the 20 countries most impacted by terrorism were all defined as being in conflict. As noted in a recent study by UN CTED, armed conflicts, particularly those of a protracted nature, and the resulting violence, instability, and breakdown of rule-of-law institutions, act as drivers of violent extremism that may lead to terrorism[25]. The number of armed groups designated as terrorist organisations engaged in various armed conflicts has increased in recent years. Some of these groups are well-armed and resourced and show relatively high levels of organisation, enabling them to carry out sustained and concerted operations.

46. In other cases, even when terrorist groups or fighters are not directly involved in a particular armed conflict, operating in close proximity to such conflicts affects their financing tactics. Several jurisdictions have reported diversion of humanitarian aid funds for TF purposes; either through sham NPOs or through the abuse of legitimate charities and NPOs which operate in crises and war zones. Profusion of weapons may also enable terrorist groups to derive profit from illicit arms trade (IAT).

47. In some cases (both armed conflict and non-conflict settings), sexual and gender-based violence (SGBV) is part of the strategic objectives and ideology of certain terrorist groups and is used as a tactic of terrorism and an instrument to increase their finance and

[24] Global Terrorism Index 2025, page 34

[25] UN CTED study on The interrelationship between counter-terrorism frameworks and international humanitarian law (2022).

© FATF-OECD 2025

power through recruitment and the destruction of communities[26]. As a source to finance and sustain terrorist activity, using SGBV can be a form of compensation and reward to fighters as well as ransoming trafficked and abducted victims back to their families[27]. UN CTED observed that the "systematic sale of Yazidi women by ISIL fighters represents the most significant known instance of the use of sexual slavery to generate revenue"[28].

1.3. Access to, or control over, natural resources

48. Access to natural resources, whether obtained through territorial control or clandestine operations, is another factor to consider. Terrorist organisations are reported to engage in highly diverse array of activities related to natural resources, such as farming, fishing, mining, and wildlife trafficking, both at production stage (e.g., operating artisanal mines, timber logging, or gold panning) and through illicit trade and smuggling activities[29].

49. 47% of the 4th Round MERs identifies access to, or control over, natural resources as a contextual factor influencing jurisdiction's financial systems and 29% specifically identifies it as a factor influencing the TF risk landscape[30]. The 2021 FATF report on Money Laundering from Environmental Crime stated that "there is evidence that armed groups and terrorist organisations do, to varying extents, rely on certain environmental crimes to support and finance their operations"[31]. Section 2 offers a more detailed analysis of the methodologies used by terrorist organisations to generate revenue from natural resources considering contextual factors enabling such financing strategies. These factors include the availability of lucrative natural resources, territorial control by terrorist organisations or weak security enforcement from authorities, weak State oversight of natural resources exploitation, and exposure to smuggling through vulnerable borders, transport infrastructure, or maritime access points.

50. In addition, access to maritime channels and facilities may be linked with piracy operations, as is the case, for example, with Al-Shabaab[32] along the Gulf of Aden and off the

---

26 UNSCRs 2242 (2015), 2331 (2016), 2388 (2017), 2467 (2019) and 2482 (2019); UN CTED report "Towards Meaningful Accountability for Sexual and Gender-Based Violence Linked to Terrorism", November 2023, page 8, available at www.un.org

27 Ibid., page 9

28 UN CTED, Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing(2019), paragraph 61.

29 See also, UN CTED Trends Alert, Concerns over the use of proceeds from the exploitation, trade, and trafficking of natural resources for the purpose of terrorist financing (2022).

30 Based on the Secretariat's analysis of 185 published Mutual Evaluation Reports (MERs) from the Global Network. While efforts were made to ensure comprehensive coverage, variations in terminology across MERs mean that some relevant references may not have been captured by the search terms used. As a result, there may be some omissions in the dataset. Nonetheless, the Secretariat considers the dataset sufficiently accurate and complete to support a robust and representative analysis. MERs available in www.fatf-gafi.org.

31 FATF Report on Money Laundering from Environmental Crime (2021), page 8. FATF also noted that environmental crime, particularly mining, is a profitable tool for insurgent groups in conflict with the central government authority and for terrorist organisations operating in resource-rich jurisdictions where there is instability. Public reporting by Governments and NGOs has noted that these groups will engage in environmental crime as a means of raising revenue or as a direct means of value transfer/payment for goods (e.g., guns and drugs).

32 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also

© FATF-OECD 2025

coast of Somalia, where the group targets cargo ships and disrupts maritime traffic to collect ransom from captured vessels[33]. Access to coastal facilities, can also be strategic for terrorist groups seeking opportunities to take control of maritime assets.

51. Water can play a role as a source or an intensifier of conflict as competition increases over scarce water resources, including for fishing and agriculture[34]. In conflict zones or fragile settings, the consequences of water shortages or severe water pollution resulting from the loss of aquatic ecosystems, such as fisheries, can lead to conflicts between different water user groups and may be used as a tool by terrorist groups to delegitimise government institutions. In Iraq and the Syrian Arab Republic, for example, ISIL has exploited water shortages and taken control of water infrastructure to impose its will on communities[35].

1.4. Weak governance, high levels of corruption and other crimes

52. Political and economic realities within States play a significant role in the close co-operation between criminal elements and terrorist organisations operations and settlements. 21% of the 4th Round MERs have identified weak governance-related matters, systemic corruption and high criminal levels as influencing the nature of TF risks in jurisdictions[36]. Furthermore, there is agreement within the literature that criminal and terrorist organisations thrive in weak, post-conflict states with ineffective legal and institutional frameworks, States experiencing widespread and systemic corruption, and States offering lucrative criminal opportunities[37].

53. Terrorist organisations often leverage and exploit weak governance as a vulnerability to move funds between countries, sustain their operations[38], and even settle their training camps and/or financial hubs. In some countries, insufficient regulatory oversight, limited law enforcement capacity, and pervasive corruption enable criminal activities that generate funds for terrorist activities to flourish unchecked. Additionally,

---

subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

33 S/2025/71/Rev.1, paragraphs 39-40.

34 UN CTED Trends Alert, (2022), pages 7-8. Concerns over the use of proceeds from the exploitation, trade, and trafficking of natural resources for the purpose of terrorist financing (2022), pages 7-8.

35 UN CTED Trends Alert, Concerns over the use of proceeds from the exploitation, trade, and trafficking of natural resources for the purpose of terrorist financing (2022), citing to Climate change "aggravating factor for terrorism": UN chief (2021), UN News, with reference to the Security Council debate of December 2021 on security in the context of terrorism and climate change.

36 Based on the Secretariat's analysis of 185 published Mutual Evaluation Reports (MERs) from the Global Network. While efforts were made to ensure comprehensive coverage, variations in terminology across MERs mean that some relevant references may not have been captured by the search terms used. As a result, there may be some omissions in the dataset. Nonetheless, the Secretariat considers the dataset sufficiently accurate and complete to support a robust and representative analysis. MERs available in www.fatf-gafi.org

37 FATF and GIABA joint report on Terrorist Financing In West Africa (2013), page 15

38 E.g., United Nations, Deputy Secretary-General, Remarks at the 2024 High-Level African Counter-Terrorism Meeting: "Strengthening Regional Cooperation and Institution Building to Address the Evolving Threat of Terrorism in Africa", 22 April 2024, Abuja, Nigeria; see also CTED Trends Alert, Counter-Terrorism and Border Management in Africa, Fundamental and cross-cutting challenges, April 2024, pages 10-11

© FATF-OECD 2025

vast spaces with limited governmental control and the lack of financial infrastructure in rural areas allow terrorist groups to establish control, levy taxes, and engage in extortion.

1.5. Porous borders

54. Porous national borders refer to jurisdictions boundaries that are not well-secured or controlled, allowing for the unrestricted movement of people and goods, often creating an ideal setting for various illegal activities. As a result, jurisdictions with either porous borders or ungoverned spaces around the boundaries lines, face heightened TF risks. The vulnerabilities may arise from natural factors (e.g., wide-ranging borders, maritime frontiers, desert or mountainous landscapes, or riverine borders where water level fluctuates seasonally), institutional weaknesses (such as inadequate border controls, ineffective customs management, a lack of checkpoints or physical barriers, and resource constraints), or political and social challenges (including territorial disputes, corruption, and limited cooperation between neighbouring jurisdictions).

55. 30% of 4th Round MERs[39] identified porous borders as a contextual factor influencing TF risks.

56. Border-related vulnerabilities can allow the movement of terrorists, as well as the exploitation of licit or illicit trading networks, the transportation of cash and illicit funds, goods, and arms used to finance and support terrorism, across land, air, and maritime borders[40]. Some jurisdictions have reported cases of cash moved across porous borders with the use of technology-enabled devices, such as drones. In addition, shortcomings in addressing the topographical, structural and resource-related limitations specific to border towns create vulnerabilities, which are exploited by terrorist groups to raise and move funds, including through trafficking and smuggling of natural resources and cultural artefacts.

57. Overall, porous borders and weak governance of border towns, villages, and regions allow transnational illicit activity, including the movement of terrorists and related funds.

1.6. Operating in the context of informal, unregulated, and cash-based economic activities

58. Economic factors, such as the prevalence of informal economy and the fact that an economy is largely cash-based can create additional vulnerabilities[41] that increase the risk of potential exploitation for TF purposes. Although informal or predominantly cash-based economies are not inherently vulnerable to TF activities, terrorists may exploit certain contextual features these economies present—such as anonymity, lack of regulation, unreported transactions, and insufficient controls over cross-border cash-flows—to support their operations and manage finances. As such, 34% of the 4th Round MERs

[39] Based on the Secretariat's analysis of 185 published Mutual Evaluation Reports (MERs) from the Global Network. While efforts were made to ensure comprehensive coverage, variations in terminology across MERs mean that some relevant references may not have been captured by the search terms used. As a result, there may be some omissions in the dataset. Nonetheless, the Secretariat considers the dataset sufficiently accurate and complete to support a robust and representative analysis. MERs available in www.fatf-gafi.org

[40] UN CTED Trends Alert "Counterterrorism and Border Management in Africa: Fundamental and Cross-Cutting Challenges", April 2024, page 8—available at www.un.org

[41] FATF/ECG(2025)4/REV1 (non-public report) on TF Risk and Context Toolkit

© FATF-OECD 2025

highlighted informal economy or largely cash-based economies as a contextual factor impacting the jurisdictions risk landscape, while 21% identified this factor as influencing TF risks specifically[42]. Findings from the TPC further underscore this point, with the private sector identifying informal economic activities as a significant vulnerability for TF, particularly due to the difficulty in applying effective CDD and transaction monitoring in such contexts.

59. The informal sector in many countries, encompasses a wide variety of small business, street vendors, and small-scale traders that rarely deal with the formal financial systems. While informal economic activities may be legal as such (unless operating in jurisdictions where unlicensed / unregistered operation is prohibited), its predominance in a jurisdiction can act as a TF risk amplifier, as informal businesses lack effective regulation, which results in greater opacity on beneficial owners. Informal economic activities are also characterised by transactions mainly conducted in cash, thereby making it difficult for authorities to trace the proceeds and establish links with terrorism. Informal economic activities may also involve the commercialisation of a mixture of licit and illicit goods, such as counterfeit products, items not subject to standardisation—such as charcoal—and smuggled commodities. These activities can generate significant cash flows that can be diverted towards TF.

60. Several NRAs in African countries identify the informal currency exchange sector, especially operating in border regions, as high-risk in terms of money laundering and TF. Some of the world's most active and dangerous terrorist groups, which operate across borders, tap into vast informal economies. In situations aggravated by conflict and instability, which create disruption in the supply and access to goods and services, vulnerabilities of informal economies and cash-based businesses may offer terrorist actors opportunities to integrate and obfuscate their proceeds-generating activities, including smuggling and trafficking, and extortion.

61. Among specific examples, ISIL-Libya has been reported to operate small and medium-sized enterprises in Sahel towns run by their sympathisers, especially in western Libya. Mozambican authorities report that Al Sunnah wal Jama'ah (ASWJ)[43] engages in fundraising through operating small grocery stores and electronic money agencies. These two activities are predominantly conducted in villages, with little formality for registrations or regulation. Similarly, ISIL operatives in Southern Africa are also reported to be operating car wash businesses and the sale of second-hand motor-vehicles, which are also highly informal and cash intensive in nature. Boko Haram is also involved in a range of informal trading activities to fund its operations. For instance, the group participates in the illegal trade in fuel whereby local fuel dealers would supply it with the crucial commodity for its mobility and operations. It has also been reported to venture into selling scrap metal and aluminium[44]. In Eastern Africa, terrorist organisations have been reported to migrate to jurisdictions with high informal economy where they engage in

[42] Based on the Secretariat's analysis of 185 published Mutual Evaluation Reports (MERs) from the Global Network. While efforts were made to ensure comprehensive coverage, variations in terminology across MERs mean that some relevant references may not have been captured by the search terms used. As a result, there may be some omissions in the dataset. Nonetheless, the Secretariat considers the dataset sufficiently accurate and complete to support a robust and representative analysis. MERs available in www.fatf-gafi.org

[43] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[44] S/2025/71/Rev.1, paragraph 105.

© FATF-OECD 2025

sham marriages to get legitimacy for investment in small businesses and for the purpose of blending in with the local population.

1.7. *State sponsorship of terrorism*

62. A variety of publicly available sources of information and delegations' inputs to this report indicate that certain terrorist organisations have been and continue to receive financial and other forms of support from several national governments. This can relate to all types of terrorist organisations, either those listed on UNSCRs and/or domestic and regional designations lists. When an organisation is not designated at the multilateral level, it is more likely to engage in financial activities, including fundraising and storing, in jurisdictions outside the reach of the sanction regime.

63. While the FATF has not developed a typology specific to state-sponsored terrorism, it has explicitly noted[45] that the funding of terrorism, or the resourcing of a terrorist entity, by any State, is incompatible with adherence to the FATF Standards and mandate, as well as the International Convention for the Suppression of the Financing of Terrorism, and paragraphs 1(a) and 2(a) of UNSC Resolution 1373 (2001). The possibility that States may choose to provide financial or other forms of support to organisations that engage in terrorist acts[46] is a longstanding TF threat to international peace and security, as well as to the stability of regional financial and political systems. Moreover, it undermines the effectiveness of FATF activities that are intended to support governments in adopting best practices to detect, deter, and otherwise disrupt TF[47].

64. Delegations reported on this trend by referring to the use of state sponsorship for TF either as fundraising technique or as part of the financial management strategy of the certain organisations engaging in terrorist acts. Several forms of support have been reported, including direct financial support, logistical and material support, or the provision of training.

65. Delegations reported state sponsorship for TF purposes coupled with sanctions circumvention techniques through trade and smuggling mechanisms where the national government potentially plays a supportive role. Trade-based money laundering (TBML) methods are used to convey value to a territory controlling organisation, with traded items for transiting through a third country to hide the real destination. Schemes involving several commodities have also been reported, with for instance oil shipped to an intermediary country to be sold in gold, with gold later converted to cash in another jurisdiction.

---

45 FATF Emerging Terrorist Financing Risks (2015), page 20.

46 See the FATF Glossary for the definition of terrorist act referred to in the introduction of the report.

47 FATF Emerging Terrorist Financing Risks (2015)

© FATF-OECD 2025

1.8. Free trade zones

66. Free trade zones (FTZs)[48] or free zones[49] are an integral part of the global supply chain[50]. They are meant to facilitate trade without a relaxation of legal requirements, especially AML/CFT controls. However, cases are documented of FTZ resulting in lesser regulatory oversight which can by exploited for illicit activities[51].

67. Vulnerabilities related to free trade zones can include opportunities for the generating or moving funds and goods by terrorist groups and their proxies or supporters and can also be a way to evade sanctions. Goods can be shipped through multiple ports or countries to hide the true origin or destination, give appearance of legality to illicit products, using false documentation, falsified shipping documents, end-user certificates, or bills of lading to misrepresent the nature of the cargo or the final recipient.

68. Some NRAs have identified these areas as inherent TF risks. For example, Malta has considered its geographical location as a transhipment hub, centre of a major trading route, its proximity to sanctioned countries as well as its Free Port as potentially vulnerable for TF[52].

2. Types of terrorist actors

2.1. Networked organisations relying on regional and domestic affiliates

69. Large-networked terrorist organisations operating in multiple jurisdictions pose specific TF risks for jurisdictions in which elements of their structures are present. Their financial resources and needs depend greatly on the network's degree of centralisation.

70. Those networked groups typically pursue active worldwide propaganda strategies, which represent a significant part of their expenses. As a result, a prominent characteristic of these networked organisations is their ability to benefit from considerable donations from sympathisers worldwide, which are raised through off-line and online campaigns, and conveyed through various vectors depending on contexts and their needs. Some

---

48 FATF Money Laundering vulnerabilities of Free Trade Zones (2010) defines Free Trade Zones as "The geographic area in which special regulatory and tax treatment is applied to certain trade-related products and services, which in this paper is referred to as a free trade zone, is also known by various other names throughout the world, including: free zones, freeport zones, port free trade zones, foreign trade zones, e-zones, duty free trade zones, commercial free trade zones, export processing zones, logistic zones, trade development zones, industrial zones/parks/areas, hi-tech industry parks, hi-tech and neo-tech industrial development zones, investment zones, bonded zones, special economic zones, economic development zones, economic and technological development zones, resource economic development zones and border economic cooperation zones"

49 World Customs Organisation (WCO), Revised Kyoto Convention (2008) defines Free Zones as "… a part of the territory of a Contracting Party where any goods introduced are generally regarded, insofar as import duties and taxes are concerned, as being outside the Customs territory", specific Annex D, Chapter 2—available at www.wcoomd.org

50 WCO, Practical Guidance on Free Zones (2020), page 4 and 8

51 Royal United Services Institute for Defense and Security Studies (RUSI), 'Free Trade Zoned and Financial Crime- A Faustian Bargain?' (2019), Anton Moiseienko, Alexandria Redi, Isabella Chase—available at www.rusi.org

52 Malta's National Risks Assessment on Money Laundering, Terrorist and Proliferation Financing and Targeted Financial Sanctions (2023).

© FATF-OECD 2025

organisations of this type have been reported to generate income from online sale of organisational products, such as t-shirts and flags with organisational signs. Terrorist entities with large networks and investments, businesses, and assets spanning multiple jurisdictions are also reported as increasingly using professional enablers (e.g., lawyers, accountants) to facilitate their financing networks.

71. Other items of expenses and sources of revenue of large-networked organisations are likely to greatly depend on their level of centralisation. Large networks can face expenditures linked to recruitment and remuneration of members and fighters, assistance to families of deceased or imprisoned fighters; payments to secure release of detainees from prisons and detention camps; training operations; as well as purchases of weapons and ammunitions. Nevertheless, such expenses can turn out limited for the core organisation if it relies mainly on regional and domestic affiliates, or loyal small cells and isolated individuals, to conduct operations.

72. Decentralisation has been one of the most reported trends regarding worldwide terrorism activities in recent years. For example, AQ over the past years used a centralised consultation council, known as Majlis al-Shura, to manage key strategic decisions, including financial management. As the organisation has progressively shifted to a de-centralised model, loose central elements are now relying on regional branches, such as Al-Qaida in the Islamic Maghreb (AQIM), Al-Qaida in the Arabic Peninsula (AQAP), Jama'a Nusrat ul-Islam wa al-Muslimin (JNIM), Al-Qaida in the Indian Subcontinent (AQIS)[53] or Al-Shabaab[54], which conduct operations and generate funds locally.

73. This trend towards de-centralisation is also salient in ISIL-core's growing reliance on some of its regional affiliates which are largely autonomous relying mostly on local fundraising operations[48]. At the culminating point of its territorial control in parts of Syria and Iraq, ISIL was able to centrally generate most of its revenue and resources through taxation, exploiting natural resources (especially gas and oil) and conducting criminal activities. In recent years, the importance of revenue generated by ISIL-branches in Africa has been especially noteworthy, as these branches are considered less vulnerable to disruption, in part due to their reliance on informal channels and illicit sources, such as KFR, abusing local populations or illicit smuggling.

74. Several "regional hubs" are now identified as playing a central part within international terrorist networks. Besides increasingly contributing to financing core organisations, those "regional hubs" gather revenue before streamlining it to fellow affiliates in neighbouring jurisdictions, to finance operations regionally. This dependence ensures the continuous affiliations of local groups and supports the promotion of core-organisations agenda worldwide.

75. According to the UN, ISIL's most successful regional financial offices include al-Karrar, al-Furqan, and al-Siddiq.

---

53 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). AQIS is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

54 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

76. Research[55] indicates that al-Karrar transfers hundreds of thousands of dollars in funds generated by ISIL-Somalia to ISIL operatives in South Africa, who transfer cash to other operatives in Kenya, Uganda, and Tanzania. The South African operatives then send the cash to ASWJ[56] and the Allied Democratic Forces (ADF)[57] and other ISIL financial offices such as al-Siddiq and al-Furqan, which oversee financial operations in Central Asia and West Africa, respectively. For example, in East Africa, to achieve such levels of financial success and sophistication, al-Karrar office made their Puntland home a hub for international operatives, with foreigners comprising around half of the current ISIL operatives in Somalia[58]. ASWJ and ADF mostly operate outside the territorial control of their respective governments. Meanwhile, operatives in South Africa take advantage of established economic structures, local corruption, and complacency to finance and provide support for international operations[59].

77. Maktab al-Furqan (the Furqan office) oversees ISIL-West Africa and other ISIL branches in the Sahel, Tunisia, Algeria, Libya, Cameroon, Niger, and Chad and provides them with operational guidance and international funding under the purview of the General Directorate of Provinces[60]. According to a May 2024 report by the US Department of Treasury[61], the ISIL branch in West Africa engages with the formal financial sector by using bank accounts to transfer money. Unlike its more successful counterpart, Maktab al-Karrar, al-Furqan is likely seeking additional income due to a lack of stable revenue. Nevertheless, it reportedly collects 50% of funds generated by the larger Islamic State West Africa Province (ISWAP) in Nigeria and redistributes them to smaller branches in the region.

78. The primary financial facilitator behind recent ISIL-K attacks is Maktab al-Siddiq (the al-Siddiq office), which oversees a large illicit financial network that raises money through donations and receives money from other regional counterparts, transferring funds much across Asia[62]. The office employs unregistered money service businesses (MSBs), established hawala networks, cash couriers, and VAs to finance subordinates in Afghanistan, Pakistan, India, Bangladesh, Maldives, and the Philippines[63]. Researchers

---

55 Global Network on Extremism and Technology, "Combating the Islamic State Finance: Somalia and Pan-African Nexus", Adam Rousselle (2025)

56 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

57 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

58 Report: IS-Somalia becomes financial hub; leader could be top IS chief (September 2024)

59 Global Network on Extremism and Technology, "Combating the Islamic State Finance: Somalia and Pan-African Nexus", Adam Rousselle (2025)

60 Global Network on Extremism and Technology (GNET), "Combating Islamic State Finance: West Africa and the Sahel (2025); Combating Terrorism Center at West Point, "The General Directorate of Provinces: Managing the Islamic State's Global Network - Combating Terrorism Center at West Point", Tore Hamming, July 2023.

61 Fact Sheet on ISIS Financing

62 Global Network on Extremism and Technology, "Combating Islamic State Finance: Central Asia and Around the World", Adam Rousselle, February 2025—available at Combating Islamic State Finance: Central Asia and Around the World – GNET

63 Fact Sheet: Countering ISIS Financing (2022).

© FATF-OECD 2025

point out that Maktab al-Siddiq is unlike its African counterparts in terms of local revenue generation, as its subordinate groups do not control significant territories. Rather than generating revenue through controlled lands, ISIL-K and other groups under the purview of al-Siddiq generate funds through more covert means such as extorsion, robbery and KRF, and increasingly rely on external funding sources expanding the geography of donations through the spread of propaganda on platforms such as Telegram, Theema, RocketChat, and others, and receiving funds in VAs[64]. At the same time, al-Siddiq is also receiving funding from al-Karrar[65].

79. Some affiliates can benefit from operational autonomy, while acting under the banner of a larger terrorist organisation. In some geographic areas, like South Asia, affiliated organisations are even observed relying on smaller proxy organisations, which are during a short lifespan conducting operations on behalf of the larger group, before disappearing.

80. Regional or domestic affiliated terrorist organisations may display TF features differing from the one observed at the level of core elements. Some affiliates may benefit from donations less frequently from international sympathisers, even though this is a potential TF risk to monitor. Their fundraising methods are typically conducted at the local level and are often associated with criminal activities, sometimes enabled by a degree of territorial control. These may include the extortion of local populations and businesses within strongholds, KFR, the exploitation of natural resources, and involvement in smuggling operations. Some regional or subregional branches of larger terrorist organisations have been also reported to use sham NPOs or abusing legitimate NPOs to collect funds disguised as humanitarian causes.

81. Despite significant expenses to conduct their operations, the extent to which regional and domestic affiliates manage to generate profit through local criminal activities or informal economic activities result in some organisations coming up with a financial surplus that can be made available to core-organisations or fellow affiliates. Furthermore, some regional affiliates that are weakened in operational terms, may re-focus on logistical activities such as financing, arms trafficking and transporting fighters to affiliates in other regions[66].

2.2. Non-affiliated regional and domestic terrorist groups

82. Groups operating at regional or domestic level without any affiliation can require significant funding to support the scope of their operations: recruitment and support of fighters, propaganda campaigns, and finance operations. Such groups rely primarily on donations from the jurisdiction or region where they operate, or from supporting members of a diaspora abroad. They rarely control any territory or passage, and typically operate with covert financing methods. Lack of affiliation implies that they do not receive funding from a core group or use significant regional financial hubs.

---

64 Global Network on Extremism and Technology, "Combating Islamic State Finance: Central Asia and Around the World", Adam Rousselle, February 2025—available at Combating Islamic State Finance: Central Asia and Around the World – GNET

65 Combating Terrorism Center at West Point, "Islamic State-Somalia: A Growing Global Terror Concern", Caleb Weiss and Lucas Webber, September 2024—available at Islamic State-Somalia: A Growing Global Terror Concern - Combating Terrorism Center at West Point

66 S/2025/71/Rev.1, paragraph 47 referring to ISIL-Libya facilitating movements of fighters to the Sahel.

© FATF-OECD 2025

83. Some jurisdictions, including those of the Latin-America region, emphasise links observed between such terrorist groups and organised crime. They also report on fundraising methods based on drug-trafficking, KFR as well as extortion from local populations. Those jurisdictions also report on cash remaining predominant method for moving and storing funds.

2.3. Ethnically or racially motivated terrorism

84. Ethnically or racially motivated terrorism (EoRMT), or as referred to by the UN non-exhaustively, "terrorism based on xenophobia, racism, and other forms of intolerance, or in the name of religion or belief"[67] represents a significant and growing global security threat. Terrorist attacks on the basis of EoRMT vary in the ideology they draw from but are often rooted in individuals and groups espousing such ideologies, and do not constitute coherent or easily defined movements but rather a shifting, complex and overlapping milieu of individuals and groups[68].

85. Given the rise of violent extremist rhetoric worldwide, which often involves scapegoating specific groups based on their race, ethnicity, gender, or other characteristics, combined with the widespread use of online social media platforms, these forms of terrorism are likely to increase in scale.

86. Violence is often perpetrated through low-cost, low-tech, copycat attacks by unaffiliated individuals or small groups, targeting soft and symbolic targets, such as places of worship[69]. Radicalisation to these types of violent actions has been become transnational, including through international travel, networking, communication and mutual inspiration through cyberspace. The phenomenon poses novel challenges, including the use of VAs for financing, gamification in recruitment efforts, an ecosystem of social media platforms and websites resilient to takedown operations, and narratives that use ambivalent and coded language to avoid being classified as unlawful speech[70].

87. Another common challenge in relation to such groups, especially where they are not proscribed or designated as terrorist or violent extremist (or not recognised as such in other jurisdictions), is that their activity, including financial activity, is not regarded as unlawful unless directly linked to a violent attack. This allows them to fundraise in overt and deliberately public ways, including through rallies, concerts and other social events, as well as public online campaigns. Sources of income may include direct donations, political grants, membership fees, mail-order or online sales—such as music, literature,

---

67 UN General Assembly resolution 75/291, 30 June 2021. Although EoRMT and XRIRB are the terms currently used by the FATF and the United Nations respectively, there is no consensus among the international community that this terminology should have universal application.

68 UNODC Manual on Prevention of and Responses to Terrorist Attacks on the Basis of Xenophobia, Racism and Other Forms of Intolerance, or in the Name of Religion or Belief, 2022, page 3—available at www.unodc.org

69 Open Briefing by the Security Council Committee pursuant to resolution 1373 (2001) concerning Counterterrorism, October 2020.

70 Report of the Secretary-General on Activities of the United Nations system in implementing the United Nations Global Counterterrorism Strategy, 29 January 2021 (A/75/729) , paragraph 11

© FATF-OECD 2025

and merchandise—the monetisation of online content, and proceeds from real estate transactions[71].

88. Such groups can also be observed taking part to offences traditional for organised criminality, including robberies, frauds, and drug trafficking. Links with motorcycle gangs and football hooligans have been regularly documented in the past years. These groups generally do not have the ability to generate funds stemming from the control of territory, such as extorting fees from population or business. However, some EoRMT groups have been reported to collect so-called "patriotic taxes".

89. Since the publication of the 2021 FATF report on EoRMT TF[72], EoRMT has expanded in scope and geographic reach, although the report conclusions related to financing trends remain largely valid as of 2025.

90. The vast majority of EoRMT terrorist attacks in recent history have been perpetrated by self-funded individuals, rarely involving complex organisation and weapons. Lone-actor attacks are often spontaneous and even involve tools already owned by the perpetrator (or, in some cases, easily accessible equipment like motor vehicles). As expenses for these attacks are low, and rarely differ from normal transactions, there are often few or no red flags in the financial system and most useful financial information is only discovered through police investigations after an attack has taken place. Furthermore, producing a broad set of indicators for international use is challenging due to the rather loose, eclectic ideology reflected in the niche terminology of different groups.

91. In terms of expenditures, many EoRMT groups can be seen dedicating significant parts of their resources to training. Members of these groups can take part in training camps in remote areas of countryside, where they can attend lectures, martial arts classes, and practice in the use of weapons. Such trainings increase the operational capability of EoRMT groups, build trust between the members, and contribute to spread their ideology. Funding is used both for the implementation of these training courses and for the equipment. Other expenditures include webhosting, production of merchandise and propaganda materials, and international travel.

92. As for the management of their funds, EoRMT groups are seen as mostly relying on bank accounts and cash. At the same time, several delegations reported that similarly to other types of terrorist organisations, EoRMT groups are increasingly turning to social media to raise donations, and to VAs to collect, store and move funds.

2.4. Individual terrorists, including foreign terrorist fighters, and small terrorist cells

93. Individual terrorists, including foreign terrorist fighters (FTFs) or small terrorist cells without direct affiliations to larger terrorist organisations, face minimal financial needs since costs of terrorist attacks are often small, and logistical or financial support from a larger organisation or network is not required. Between 2014 and 2023, several regions—including Europe and North America—experienced a marked increase in terrorist attacks perpetrated by individuals affiliated with specific ideologies. While

[71] Security Council Committee established pursuant to resolution 1373 (2001) concerning counterterrorism, Global survey of the implementation of Security Council resolution 1373 (2001) and other relevant resolutions by Member States, November 2021 (S/2021/972), paragraph 668 —available at www.un.org

[72] FATF Ethnically or Racially Motivated Terrorist Financing (2021).

© FATF-OECD 2025

sometimes inspired by one or more terrorist organisations, these individuals often acted independently and were not formally linked to any particular group[73].

Foreign terrorist fighters[74]

94. Unlike lone terrorist actors, FTFs usually affiliate themselves with a terrorist organisation which they ultimately seek to join in the area it operates, and in most cases some of their expenditures are covered by such organisations in the form of regular payments or provisions in kind, especially during the time when they actively fight or serve other functions for the organisations. At the same time, some of the financing methods employed by FTFs, especially as they prepare their departure to the area of operation, are similar to those used by individual terrorists who do not travel to join a terrorist organisation.

95. By 2014, the flow of FTFs to ISIL-controlled territories in Iraq and the Syrian Arab Republic reached unprecedented levels. Estimates suggest that more than 42,000 individuals from more than 120 countries travelled to join terrorist organisations at that point[75]. By early 2018, thousands of FTFs had left the conflict zones in those countries, but the fate of a large proportion of the ISIL FTF contingent remains unknown: there is a large discrepancy between the total number of FTFs and those recorded as having been killed or detained or having returned or relocated. As of 2025, one emerging theme is the regional nature of FTF recruitment in the conflict zones in Africa. Throughout 2024, ISIL in Somalia experienced a rapid growth in FTFs, which nearly doubled the size of the group, although seemingly slowing down due to difficulties in integrating fighters and other factors[76]. Several jurisdictions also noted an increase in FTFs travelling to Afghanistan[77]. With the evolving situation in Syria, there are reports of ISIL potentially strengthening the FTFs' presence there[78].

96. Initially, FTFs expenditures focused on covering travel costs, living expenses in conflict zones, purchasing weapons, other operational equipment to be used in combat and medical support. Over time, these financial expenditures shifted towards sustaining individuals who move between conflict zones, remain in detention camps (particularly, ISIL-related FTFs and associated individuals), or return to their countries of origin (including reintegration costs)[79]. There is also a noticeable trend of larger sums being sent to returning FTFs, often used for handover to terrorist groups before departure, or to pay traffickers and smugglers[80].

---

73 Global Terrorism Index 2025, page 38.

74 In UNSCR 2178(2014), FTFs are defined as "individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict".

75 UN CTED 2024 Trends Tracker on Evolving trends in the financing of foreign terrorist fighters activity 2014-2024

76 S/2025/71/Rev.1, paragraph 37

77 See also S/2025/71/Rev.1. paragraphs 88-89 on ISIL-K FTF recruitment.

78 S/2025/71/Rev.1, paragraph 57; see also Section 3.

79 FATF Emerging Terrorist Financing Risks (2015), page 24; EAG, *Mutual Evaluation Report of the Republic of Kazakhstan*, paragraph 529—available at www.fatf-gafi.org

80 UN CTED 2024 Trends Trackers; APG Yearly Typology Report, "Methods and Trends of Money Laundering and Terrorism Financing" (July 2022), page 21; FATF Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling (2022), page 28.

© FATF-OECD 2025

97. Financial activity linked to FTFs typically involves supporters collecting or sending small amounts of money abroad or financing travel to zones with terrorist activity. This money often comes from legal means, including personal savings, and may sometimes be collected on behalf of others. Individuals may coordinate the donations through encrypted mobile applications, send the funds in the form of VAs, transfer them abroad through a fiat MSB, or, carried in cash and handed over to couriers. Overall, the financial patterns associated with FTFs have demonstrated remarkable adaptability, shifting from simple methods of fund transfers to increasingly sophisticated and technologically advanced approaches[81].

98. Research indicates that funds are now frequently used to establish new networks in different conflict zones[82] including by bribing local officials or community leaders for protection or information and integrating into new cells[83]. Moreover, there is an enhanced focus on technology and communications, with increased investment in secure communications devices, software, and cybersecurity measures, reflecting the broader trend of terrorist groups prioritising technological resilience and operational security[84].

99. Some trends specifically relate to returning FTFs. These include covering costs related to individual reintegration[85] and/or, on the contrary, covering costs related to maintaining ideological connections, such as funding small-scale propaganda efforts or ideological materials, supporting online platforms for communication with like-minded individuals[86]. Additionally, there is often continued financial support for individuals left behind in conflict zones[87].

100. Specifically in relation to ISIL-associated FTFs, financial flows are observed originating from jurisdictions of origins of FTFs, towards prison camps in the Iraqi-Syrian region in order to smuggle-out or sustain-in ISIL affiliates, and/or their family members.

Small terrorist cells and lone terrorists

101. For many jurisdictions, the primary counterterrorism focus has since shifted to endogenous threats from small cells and lone actors planning local asymmetrical attacks. Indeed, ISIL's decline in the Iraq-Syria area has weakened its ability to project terrorist groups abroad, thus the terrorist group has focused its propaganda efforts on trying to

81 UN CTED 2024 Trends Tracker.

82 UN CTED 2024 Trends Tracker; APG and Global Centre on Cooperative Security, "Financing and facilitation of foreign terrorist fighters and returnees in Southeast Asia", page 10; and United Nations Office on Drugs and Crime, Foreign Terrorist Fighters – Manual for Judicial Training Institutes, Middle East and North Africa (Vienna, April 2021) www.unodc.org.

83 Audrey Alexander (Combating Terrorism Centre, West Point), "Cash camps: financing detainee activities in AlHol and Roj camps", September 2021—available at www.ctc.westpoint.edu

84 Abbud Mahmoud, "The impact of technology on conflict resolution in Syria", Journal of Conflict Management, vol. 2, No. 1 (April 2023).

85 Adam Hoffman and Marta Furlan (Program on Extremism, George Washington University), Challenges Posed by Returning Foreign Fighters (2020); and Austin Doctor and others (National Counterterrorism Innovation, Technology, and Education, University of Nebraska, Omaha), "Reintegration of foreign terrorist fighter families, a framework of best practices for the US", March 2023.

86 UN CTED 2024 Trends Tracker; Mohammed Shoaib Raza, "The silhouette of Indonesia's foreign returned terrorist fighters", Issue Brief of Manohar Parrikar Institute for Defence Studies and Analyses (New Delhi, May 2023) page 4—available at https://idsa.in/issuebrief

87 UN CTED 2024 Trends Tracker; FATF Emerging Terrorist Financing Risks (2025), pages 27-28; EAG, (EAG) Kazakhstan Mutual Evaluation Report (2023), paragraph 529

© FATF-OECD 2025

incite followers around the world to commit attacks in their own country. This is also the case with many other types of terrorist organisations and ideologies that provide inspiration to individuals or cells that they are not directly connected with.

102. Those actors present unique challenges in terms of fundraising, logistics, and operational patterns. Small cells and lone individuals typically do not rely on territorial control or access to natural resources but instead operate with lower financial needs, resulting in discreet financial activities. Their expenditures generally include basic procurement for low-scale attacks (e.g., weapons, ammunition, vehicles, dual-use chemicals, 3-D printers), propaganda materials, and donations or contributions to larger organisations, among other methods. As far as operational needs go, jurisdictions commonly describe a trend toward less-sophisticated attacks, with bladed-weapons or motor-vehicles replacing firearms.

103. Due to their smaller operational scale, these individuals can rely on legitimate sources of revenue (salary, savings, social benefits, support from relatives, small credit loans) as well as petty crimes. The fact that individuals' financial activities often occur in small amounts, and through channels not registered in their own names but rather of those of relatives, friends, or fellow community members, makes detection even more challenging for authorities. As small cells and individuals often rely heavily on revenues generated from legitimate activities, they continue to store a significant portion of their funds in basic deposit accounts. In similar fashion to other contexts, online banking services are increasingly observed in cases involving small cells and individuals. The relatively small amounts handled by these actors continue to make cash a convenient option.

104. Still, some early indicators of TF from lone actors can be identified, among which sudden changes in financial activity, like the adoption or increased use of financial channels allowing to dissimulate the origin of funds or the ultimate beneficiary of the transaction—peer-to-peer (P2P) transfers, ATM withdrawals, third party payment processors or prepaid cards. The emergence of frequent unexplained cash deposits, especially if it does not fit with the economic situation of the individual (i.e., known to be unemployed, cash deposits appearing in addition to regular pay checks), may indicate that the individual is working with a wider network[88].

105. Also, as several jurisdictions report on increasingly young terrorist individuals, cases involving minors are set to become more frequent[89]. It is then likely that revenues and financing vectors would not be nominally assigned to the individual. The financial dependencies of minors on guardians or community members may further obscure the origin and purpose of funds, complicating legal attribution and enforcement actions.

106. Small terrorist cells and individuals can provide financial contributions to larger organisations through transnational donations, using methods to move funds such as hawala, transfers through MVTS, or cross-border physical movements of cash. While traditional fundraising techniques remain prevalent, digital technologies are increasingly being used and facilitated by social media platforms, encrypted messaging applications, which allow terrorists to recruit anonymous donors, give instructions on how to proceed[90], or transmit payments for planned or executed attacks. Overall, jurisdictions dealing with

88 FinCEN Advisory, FIN-2025-A001, April 1, 2025

89 See also S/2025/71/Rev.1, paragraphs 77-78, 98 reporting on young, radicalized individuals in Europe and South-east Asia, often minors, with direct or indirect connections with ISIL through online encrypted messaging platforms; Section 3.

90 FATF Opportunities and Challenges of New Technologies for AML/CFT (2021)

© FATF-OECD 2025

terrorist threat from isolated individuals or small cells observe a growing ease from targets at using VAs and other innovative digital solutions.

3. Other considerations

3.1. Exposure to terrorist propaganda

107. For terrorist organisations, propaganda is often both a core activity and a significant expenditure. It serves multiple purposes, including expanding their support base, legitimising their actions, and intimidating adversaries. In many cases, propaganda also aims to support financing efforts—by recruiting donors and disseminating instructions on how to contribute financially. These finance-oriented communication campaigns may be carried out through a variety of channels, including social media platforms, messaging applications, traditional media, and in-person outreach, as further detailed in Section 2.

108. Exposure to terrorist propaganda may vary depending on a range of factors, including language. For example, ISIL-K maintains a highly active propaganda campaign that targets both regional and international audiences. Regionally, ISIL-K disseminates content in several Central Asian languages, including Pashto, Dari, Tajik, Uzbek, Urdu, and Farsi. Concurrently, the group also produces material in Russian, Arabic, and English, thereby expanding its reach to a broader global audience. This multilingual approach enables ISIL-K to engage not only individuals within the region but also members of the Central Asian and Russian-speaking diaspora across a wide range of jurisdictions. Al-Siddiq raises money by soliciting donations through its propaganda channels, including the Voice of Khorasan magazine, which its subordinate, al-Azaim Media Foundation, publishes in multiple languages on a monthly basis[91]. Each issue of the magazine includes an advertisement soliciting donations from readers in Monero with obscured transaction details that make it especially difficult for international authorities to detect[92].

3.2. Internal financial management structures

109. Internal financial management structures can vary widely from one terrorist organisation to another. Understanding these financial structures, is essential for disrupting their financing channels.

110. As noted above, organisations operating at a significant scale often set-up formalised accounting capacities and resort to other specialised financial management techniques. For example, Mozambique discovered in Cabo Delgado notebooks kept in Ahlu-Sunnah Wa-Jama homemade banks, indexing the group's resources and transactions. Pakistan indicates that Tehrik-e-Taliban Pakistan (TTP) designates a central financial

[91] Global Network on Extremism and Technology, "The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing", Animesh Roul, October 2024—available at The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing – GNET

[92] Global Network on Extremism and Technology, "Combating Islamic State Finance: Central Asia and Around the World", Adam Rousselle, February 2025—available at Combating Islamic State Finance: Central Asia and Around the World – GNET "Perspectives: ISKP intensifying online propaganda targeting Russia and Central Asia", Lucas Webber and Louise Meloy, September 2024—available at Perspectives: ISKP intensifying online propaganda targeting Russia and Central Asia | Eurasianet

© FATF-OECD 2025

manager, while Germany indicates that the Kurdish Workers Party (PKK)[93] employs regional managers to oversee financial operations, and the United States reports that Hamas[94] relies on key financial facilitators in foreign parties' jurisdictions.

111. Some groups still display strong centralised structures, like Al-Shabaab[95] which has established a structured financial department, or ADF[96] and the ISIL groups operating in Central Africa which centrally coordinate fund-generation and spending. In the case of Ansar al-Sunna, financial management is the prerogative of the overall commander. As previously noted, some groups are increasingly adopting more decentralised models of financial management. In such cases, the core leadership is not directly involved in the generation of funds or the oversight of operational expenditures. Instead, financial responsibilities are largely delegated to regional affiliates, who manage resources with a significant degree of autonomy. Some organisations can rely on even more decentralised structures, including collectors established in various jurisdictions and acting on small-scale basis.

112. There are also cases where financial activities are externalised, often through collaboration with organised crime networks. For example, the Taliban has been reported as hiring professional money launderers for worldwide management of their assets, including through a network of decentralised bank accounts, front companies, and cash storage sites. In cases of EoRMT groups, financial management can be centralised through specific associations. In contrast, small cells and lone actors typically self-manage their finances independently.

3.3. Gender perspective

113. A gender-sensitive approach to understanding TF risks and trends is important for developing informed and comprehensive responses[97]. Many NRAs tend to overlook this dimension, often leading to gender-blind CFT response measures.

114. Gender-blind, or conversely gender-biased, assessments may lead to false assumptions in analysing gender roles in TF and thus miss the real risks. For example, due to ill-informed profiling practices or risk indicators, women and girls may be subject to less control at borders, and thus become more frequently used as cash couriers, or their money transfers may be less scrutinised. In this regard, women have been increasingly involved as logistical and financial facilitators of FTF activity in some regions, including

---

93 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

94 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

95 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

96 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

97 For further details, see, when published, the Guidance Note on Ensuring respect for human rights while taking measures to counter the financing of terrorism.

© FATF-OECD 2025

South-East Asia[98]. Researchers also indicate that terrorists have used female names (and members) to conduct financial transactions as a basic form of tradecraft, assuming that these names would arouse less suspicion. An ISIL-affiliated brigade operating in Al-Hawl camp in Syria, comprising women engaged in intelligence gathering, youth training for operations, recruitment, and financial management, is reported to have been reactivated[99].

115. A number of online fundraising campaigns have been launched in support of family members associated with ISIL fighters detained in camps or prisons, stating that the funds are to be used to improve their detention conditions or to secure their release. Many of these campaigns claim to focus on foreign women and their children, but the raised funds are often used to support fighters (male or female).

116. The continuing abuse by terrorists of informal remittances and mobile money to transfer funds, which in some parts of the world are the only financial instruments women can use since they are not able to open bank accounts, puts them at risk of being involved, unknowingly or unintentionally, in TF activities.

117. In the past few years, women in the Middle East and North Africa have started to turn to VAs trading as a way of sidestepping the challenges stemming from local cultural norms, biased laws and algorithms, and even untrustworthy banking and financial systems[100]. Furthermore, seed crowdfunding is one method that women are using to bypass traditional financial gatekeepers and raise capital directly from funders. However, many States fail to effectively and proportionally regulate these new technologies, including for AML/CFT purposes, and to raise awareness of the service providers and users, both male and female about potential risks, which in turn may put users at greater risk of becoming victims or unwilling facilitators of TF-related activities.

118. Finally, CFT measures that are in principle gender-neutral may have discriminatory effects in practice. For example, CFT measures aimed at protecting NPOs may disproportionally affect women's rights organisations in terms of access to funding; and in some instances, they may lead to reluctance of donors or financial service providers to fund assistance programs. With respect to targeted financial sanctions, women whose family members or spouses are listed for asset freezing purposes may not have independent access to work, bank accounts or independent sources of income or the ability to own property[101].

[98] UN CTED, Launch Discussion on Trends Tracker "Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014 – 2024", November 2024—available at www.un.org/securitycouncil

[99] S/2025/71/Rev.1, paragraph 59

[100] UN Human Rights Special Procedures, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2023), position paper on International Human Rights Law Considerations for Counter-Terrorism Financing Regulation of Crowdfunding, Virtual Assets, and New Payment Technologies.

[101] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/46/3, paragraph 13 and 16

© FATF-OECD 2025

Section 2: Methods used to raise, move and manage funds and other assets for terrorist financing purposes

119. The present section aims at providing a comprehensive overview of current TF risks and trends, understood as methods used by terrorist organisations and individual terrorists to raise, move, store, or use funds and other assets. Where applicable, the section attempts to link methodologies to certain contextual or operational factors analysed in Section 1. For the sake of clarity and systematisation, these methods are each analysed separately. However, in practice, TF schemes frequently combine several techniques and channels.

1. Methods based on cash

120. Across all jurisdictions and independently of contextual factors, the use of cash remains a prevailing method for terrorist organisations and individuals to raise, move, store, and spend funds or other assets.

121. Cash is also very often used in combination with other medium, such as MVTS, VAs, mobile money, financial services. In many cases, funding raised and moved through different methods will ultimately be converted to cash to allow for anonymous payments for logistical and operational expenditures such as the payment of salaries, procurement of equipment, or financial support to families. The use of multiple channels ultimately involving cash makes it difficult to determine the final beneficiary of the funds and to track financial flows[102].

122. The reliance on methods based on cash for TF can be attributed to several factors, including the preference for anonymous payments and fund-storing methods, its universal acceptance, the lack of transaction records, limited availability of financial services in certain areas, porous borders that allow for uncontrolled movement of people and funds (including limited impact of existing cash thresholds for transport or declaration), prevalence of informal economies, among others. Cash also plays a prominent role in organised crime activities—including drug and human trafficking—so growing convergence between other forms of criminality and TF should contribute to maintain cash as a predominant channel.

123. Terrorist organisations and individuals in diverse contexts can be observed trying to raise funding in the form of cash. Groups can exploit cash-intensive businesses, whether those are legitimate or taking place informally. Among sectors exposed to such risks, it is worth mentioning retail shops, grocery stores, markets, filling stations, transport and trading companies. In a notable example in the transport sector, a business involved in the transportation industry in Kenya has been designated under the US OFAC list for financing

[102] FATF Risk of terrorist abuse in Non-Profit Organisations (2014), page 97

© FATF-OECD 2025

of Al-Shabaab[103]. Cash-based businesses as grocery shops and second-hand car markets have also been used to raise funds by ASWJ[104] in Mozambique.

124. Another method for organisations and individuals to raise cash consists in selling personal items. For instance, individuals may sell assets shortly before travelling to a conflict area or before an attack, in order to generate funds. In 2019 attack on a famous hotel in Kenya, one of the Al-Shabaab[105] attackers sold personal property the day before the attack, ostensibly to raise funds. Such methodology is a specific feature of FTF and lone actors overall.

125. More generally, many fundraising methods analysed in this report ultimately generate profit in the form of cash. For example, in kidnapping cases, the ransoms are generally required in cash; in extortion activities, fees are also being required in cash. As an illustration, the illegal taxation of truck drivers plying the routes controlled by Al-Shabaab[106] in Somalia is exclusively made in US dollars. The sale of spoiled natural resources or smuggled goods mostly occurs in the form of cash. Jurisdictions in Latin America also report that domestically designated terrorist organisations primarily mobilise funds through cash extortion.

126. Besides extortion of local population, some terrorist organisations can also aim at collecting cash remittances from diaspora located in a third jurisdiction, including through coercion. For example, one of the PKK[107] main sources of revenue are the groups' "Kampanya", consisting in collecting contributions from Kurdish diaspora and Kurdish businesses in third jurisdictions, often using intimidation or coercion. It usually takes the form of cash collection, ultimately transferred to PKK regional management through couriers. Hamas[108] has been reported to call for cash donations through diasporas as well.

---

[103] US Department of Treasury. *Treasury Designates Transnational Al-Shabaab Money Laundering Network,* March 11, 2024. Treasury Designates Transnational Al-Shabaab Money Laundering Network | U.S. Department of the Treasury. Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001); Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[104] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[105] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[106] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[107] Organisation designated under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[108] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

© FATF-OECD 2025

127. For reasons noted above, cash is also frequently used by terrorists to move funds across jurisdictions. Physical cross border transportation of cash continues to be reported as a prevailing method used to move funds, including on the African continent, in Yemen, Iraq and Syria and South-East Asia[109]. These regions mainly rely on informal, cash-based economies and have porous borders which limit monitoring of cross-border cash movements. In 2021-2022, although reduced in total amounts (from the range of USD 90,000 per month to closer to USD 40,000 or less) cash payments were reported to be regularly couriered into the Syrian Arab Republic from neighbouring States, with ISIL cells receiving reduced payments monthly[110]. Research indicates that cash couriers—some intimately affiliated with ISIL-K and others employed episodically—are likely to be used to move cash across Afghanistan and regionally[111]. Several jurisdictions also reported physical transportation of cash through borders, the use of cash couriers, and cash smuggling as predominant method to move funds by Hamas[112].

128. One of the prevalent methods for moving funds is cash couriers. Terrorists and their associates often carry cash across borders to avoid detection by financial monitoring systems, especially when done in under-threshold amounts or with false declarations. Cash may also be hidden within transported goods, such as livestock, agricultural products, and merchandise to disguise the financial transfer. For instance, in the Horn of Africa, hand-carried cash transfer is conducted using donkeys, pedestrian crossings, bicycles, trucks, passenger luggage, among others. This mode of carriage makes it very difficult for authorities to detect, hence offering a preferable method for terrorist groups.

129. Some terrorist groups share routes with organised criminal groups as these channels are ideal for obscuring the origins and destinations of funds. Criminal migration routes, goods transportation networks, and other goods cross-border exchange may be used for discreet transactions in exchange for cash. Some jurisdictions report on the increasing use of drones to carry cash across borders.

130. Cross-border transportation of cash and BNIs relating to transit passengers on cruise ships can also represent a TF-related vulnerability, and is often overlooked in NRAs[113], as they might not be subject to systematic and rigorous customs or immigration controls (including cash declaration) when entering or exiting a transit jurisdiction.

131. Cash reserve is still the main method used by terrorist networks to store values. Cash reserves can ensure discretion, liquidity for immediate operational needs and can facilitate funding activities while circumventing regulated formal financial systems or in areas where formal financial services are not easily accessible. As mentioned above, after suffering territorial loss in Syria and Iraq, where it used to store cash reserve, it is believed that ISIL hid deposits underground and subsequently dug them up. Other organisations have been described building their own saves to store cash, such as ASWJ[114] in

[109] UN 1267 Monitoring Team

[110] Organisation designated under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[111] Project CRAAFT,The Islamic State in Afghanistan: A Golden Opportunity for a 'Golden Child' Stephen Reimer, Research Briefing No. 13, (2023).

[112] Organisation designated under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[113] Fiji MER, October 2016.

[114] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored

© FATF-OECD 2025

Mozambique. In contexts of small cells and individual terrorists, small amounts of cash can easily be stored at home.

132. There is also an emerging trend where terrorist groups leverage on exchange rates to store value in stronger and less volatile currencies especially in West and Central Africa, where terrorist networks prefer exchanging local currencies with euros. Once converted into foreign currencies, it then becomes convenient to physically transport it even for large sums. In Southern Africa, ISIL has also been reported to engage in illegal exchange of foreign currency. Hence, storage of funds in foreign currencies can provide terror networks with the advantage to profit from exchange rate valuations earning additional revenues.

133. Israel reports that money changers who convert cash for Hamas[115] and the Palestinian Islamic Jihad[116] do not use banking systems, but register the money transfers manually and use offsetting methods (i.e. hawala) to transfer money.

2. Methods based on money value transfer services (MVTS)

134. MVTS providers play a critical role in facilitating cross-border fund transfers, especially in areas where formal banking services are limited or unavailable and among populations who may struggle to access financial services, such as refugees or women. In some regions, MVTS may represent the only accessible or reliable means of financial services to transfer cash or other monetary instruments. Also, transfers through MVTS can in some cases remain cheaper than wire-transfer through mainstream banks and is often the preferred option to send low amounts without incurring significant fees. Additionally, MVTS offer more flexibility with lesser regulatory requirements that are often associated with banking services such as the requirement to open accounts.

135. Similar factors also explain why MVTS are attractive for terrorist organisations and individuals. In addition to those, terrorist actors can exploit insufficient customer due diligence (CDD) by some MVTS providers and agents, allowing to disguise the real initiators or beneficiaries of transfers. This includes situations when the service provider fails to report suspicious transactions; when a complicit remitter (individual or legal person) acts as a front for a transfer; or when complicit MVTS agents connive with terrorist organisations.

136. Those vulnerabilities are particularly salient where jurisdictions display weak regulatory frameworks or supervisory capacities. They can also be combined with the use of fake or stolen documents, or the provision of incorrect data, to further dissimilate real stakeholders to the transfer. Another vulnerability comes in where the threshold of funds that can be transferred in each platform is below the AML/CFT regulations threshold, which undermines detection of potentially illicit transactions.

137. In 2015, FATF reports on ISIL financing and on emerging TF risks already highlighted typologies on MVTS abuse for TF purposes. As of 2025, nearly all terrorist groups identified have been reported to rely, at least to some extent, on MVTS to transfer

by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[115] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[116] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

© FATF-OECD 2025

funds across jurisdictions. Reports indicate that terrorist groups also frequently use MVTS to move money internally within the organisation, and to manage payments to foreign terrorist fighters, including for purposes of recruitment, travel or sustaining their stay and operations[117]. In such cases, MVTS can be used through multiple small transactions and by mixing cash methods with formal banking services.

138. The use of MVTS is also noted in the context of proceeds of crime involving cross-border transactions, such as drug trafficking, smuggling and exploitation of natural resources along with other payment methods. ISWAP is one such group that has extensively used a combination of hawala and online remittances to transfer proceeds of crime derived from natural resources and smuggling across multiple jurisdictions in West Africa.

139. Another context of abuse of MVTS by terrorist groups is for facilitating payments. Terrorist groups, such as ISIL, Boko Haram, and Al-Shabaab[118], have been reported to demand payment of ransom through both formal and informal MVTS. Diasporas' financial contributions, which can be obtained through intimidation or coercion, can also be ultimately channelled to terrorist organisations operating in another jurisdiction through MVTS.

Case study: "Time Window" modus operandi to transfer funds through MVTS

In 2020, a Spanish young man was arrested for disseminating ISIL-related propaganda campaigns. While the initial financial investigation yielded limited results, a subsequent search of his property and digital devices uncovered evidence that substantiated his involvement in ISIL's financial network.

The investigation revealed that the suspect had received instructions via a private chat with an ISIL member based in a Syrian refugee camp on how to raise and transfer funds. Acting on these instructions, he collected funds using MVTS and PayPal and transferred them from Spain to individuals in a jurisdiction neighbouring Syria. These transactions were conducted via MVTS and VAs (notably Bitcoin), using the identity of his mother. He also assisted and persuaded individuals in other countries to send funds, guiding them through the process.

Funds sent via MVTS were initially received by frontmen located in a country bordering Syria. These intermediaries would operate within a brief, predefined timeframe ("time window"), after which a new individual would take over the role to ensure continued fund transfers. Ultimately, the funds were directed to ISIL-controlled refugee camps in Syria.

[117] FATF, GIABA and GABAC joint report on Terrorist Financing in West and Central Africa (2016)

[118] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

When transferring the funds through MVTS, the recipients of these funds were based in a neighbouring country to Syria and acted as frontmen for the organisation for a short period of time. After this short period of time, the recipient was changed to another person to continue channelling funds. The final destination of these funds was a detention camp located in Syria. Several red flag indicators were identified in the suspect's financial behaviour, including links to prior terrorist activities or associations with foreign terrorist fighters, and social media activity reflecting extremist ideologies. The suspect opened multiple financial accounts—including bank accounts, prepaid cards, and e-wallets—under his mother's name, used various branches and cashiers to conduct small-denomination transactions, and regularly transferred funds to jurisdictions with heightened terrorist risks.

In 2022, the Spanish National Judicial Court sentenced him to two years and six months in prison and imposed a EUR 1,300 fine for TF.

The suspect maintained online contact with individuals in the EU, Kuwait, Germany, and Canada through platforms such as Telegram, Reddit, and Discord. These interactions led to further arrests and the dismantling of additional segments of the financing network operating similarly in the EU and Canada.

Source: Guardia Civil, Spain. (See: www.interior.gob.es; and the public conviction here www.poderjudicial.es)

140. Also, while MVTS are still frequently used by terrorists, and on a similar scale over the past ten years or so, it seems that the traditional incumbent operators now face competition from alternative operators that can be accessed exclusively online, who are more flexible, less expensive, and may be very popular with certain diasporas. Some jurisdictions note that terrorist financers tend to move away from major MVTS providers to newer, smaller or regional ones (e.g., M-Kesh, e-Mola, Taaj, Juba Express, and Mama Money in Africa) or mobile e-money providers (e.g., M-Pesa and Alipay in Asia).

2.1. Unlicensed remittances, hawala and other similar service providers[119]

141. Hawala and other similar service providers (HOSSPs)[120] are a non-formal financial system, which historically emerged as a way to facilitate trade. It is used to transfer money through a network of mediators ("hawaladars") and is widespread in particular in the Middle East, several regions of Africa and South Asia. The prevalence of HOSSPs is precipitated by the lack of formal financial services, especially in remote or conflict areas,

[119] FATF report on The Role of Hawala and Other Similar Service Providers in ML/TF (2013).

[120] According to the FATF General Glossary definition, Hawala and other similar service providers are considered a subset of MVTS. Their classification varies across jurisdictions, depending on the legal framework. They may operate as licensed/registered entities or as an unregulated or even illegal remittance mechanisms. Although the term "Hawala" is commonly used in several countries, it is not universally recognised. Therefore, for the purpose of this report, the term "Hawala and Other Similar Service Providers (HOSSP)" will be used. HOSSPs are characterised by the services they offer rather than their regulatory status. What distinguishes them from other money transmitters is their reliance on non-bank settlement methods, including settlement via trade and cash, as well as prolonged settlement period. See: FATF, The Role of Hawala and Other Similar Service Providers in ML/TF (2013), page 9.

© FATF-OECD 2025

or by restrictive regulatory policies in the financial sector, consequently driving funds transfer into the informal channels. Hawala systems charge significantly lower fees for transfers than other methods, making its usage one of the preferable methods for transferring money in many developing economies. Additionally, hawala offers highly rapid transfers when compared to formal financial transfer systems partly due to the lack of administrative procedures. This system is also common among certain communities that rely on this method due to traditional cultural practices, and to certain geographic areas.

142. When based on account settlement mechanisms, underground banking services-operating as parallel money transmitters systems which keep records of transactions and accountancy with the goal of bypassing the regulated financial sectors, can be considered as part of the HOSSP framework[121].

143. The main drivers for the abuse of HOSSP for TF is the will to escape restrictive foreign exchange controls, strict regulatory controls by some governments and steep fees charged by other financial services providers. The vulnerability of HOSSP systems for TF lies in the difficulty of tracing the parties involved due to lack of documentation, stolen, and fake identity documentation, which offers full proof anonymity, making it less risky for criminals compared to financial services leaving clearer footprints. It can also be exploited by terrorist actors to avoid exchange, capital, or administrative controls.

144. In the context of TF, HOSSPs remain among the most prevalent means of transfer of funds in many parts of the world, and more and more frequently in combination with other methods. According to researchers, ISIL-K operatives based in Jalalabad and Kabul make use of hawaladars in these cities to receive (and possibly also send) funds across international channels, as well as to help store tens of thousands of dollars on behalf of the group. These hawala networks are linked up with broader ISIL financial networks such as the so-called Al-Rawi Network, which now supports ISIL financial facilitation through operations in several countries across the globe[122].

145. In terms of TF, HOSSP[123] are mainly used for funds transfer, often in combination with other channels such as cash, mobile money, and bank accounts. However, some jurisdictions, including in East Africa, reckon that hawala usage is declining as methods such as mobile money, which are considered faster and more reliable, and cash couriers can be preferred.

146. In another context, hawala system is used to mobilise revenue particularly from diaspora sympathisers, collection of ransom, and illegal taxes. Terrorist organisations such

[121] FATF Professional Money Laundering (2018)

[122] Project CRAAFT, The Islamic State in Afghanistan: A Golden Opportunity for a 'Golden Child' The Islamic State in Afghanistan: A Golden Opportunity for a 'Golden Child'", Stephen Reimer, Research Briefing No. 13 (2023); Jessica Davis, 'ISIL's Al-Rawi Network', Insight Intelligence, 27 April 2023; US Department of the Treasury, 'Memorandum for Department of Defense Lead Inspector General', 4 January 2021; US Department of the Treasury, 'Treasury Designates Key Nodes of ISIS's Financial Network Stretching Across the Middle East, Europe, and East Africa', 15 April 2019.

[123] FATF The Role of Hawala and Other Similar Service Providers in ML/TF (2013): *"HOSSPs are defined as money transmitters, particularly with ties to specific geographic regions or ethnic communities, which arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time".*

© FATF-OECD 2025

as ASWJ[124], ADF[125], Al-Shabaab[126], and Hamas[127], have been reported to use alternative remittance systems in combination with mobile money to collect donations from migrants abroad. In West Africa, Boko Haram is reported to rely on the use of hawala to collect funds from international networks which they withdraw in cash to finance their activities[128].

147. The use of HOSSP can also be viewed as a means of settlement where terrorist networks pay for goods and services such as weapons and proceeds of illicit trading in natural resources using this method. A case in point is the reliance on hawala by ISIL's affiliate in Mozambique ASWJ[129] to transfer proceeds of the exploitation of natural resources, such as minerals and precious metals.

148. With respect to Afghanistan, UNODC has highlighted several factors that contributed to substantial impact of the Taliban takeover on the country's MVTS and HOSSP sectors, resulting in the increased vulnerability of hawaladars in Afghanistan to misuse for criminal or terrorist purposes[130].

149. HOSSPs are also evolving to integrate new solutions offered by digital innovation, and terrorist organisations are seizing the opportunity. There are reports of large and networked terrorist organisations using digital adaptations of the traditional hawala system for cross-border pseudo-anonymous transfers through blockchain. Several jurisdictions also reported that ISIL sympathisers have started using digital hawala applications which can only be downloaded upon referral by a trusted existing user. That means that such networks can be used by a closed circle of customers and therefore challenging to access by investigators. The application links the initiator with the person who will make funds available in another jurisdiction, and payments are made based on

[124] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[125] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[126] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[127] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[128] FATF, GIABA and GABAC joint report on Terrorist Financing in West and Central Africa (2016)

[129] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[130] UNODC, The Hawala System: Its operations and misuse by opiate traffickers and migrant smugglers, 2023, page 79—available at www.unodc.org

© FATF-OECD 2025

the codes and links coming from the application. Nevertheless, the use of VAs by HOSSPs seems to be limited still[131].

150. Research[132] indicates that HOSSPs are based on the same principles as the blockchain: trust, community, privacy, and decentralisation. The blockchain can be used to improve the efficiency and speed of hawala using digital processes. Blockchain can be applied to be a natural evolution for hawala, considering that in the next ten years, over six billion people are estimated to be online. According to the cited research, in a VA blockchain the nodes can be seen as hawaladar, where nodes and miners maintain the network through mutual trust and consensus. The coins received from the hawala system can be spent by using the "crypto wallet" provided by the mobile messenger app, where the purchaser can send money to the seller in any shops, without the need to exchange the currency. Depending on the type of VA used, a certain degree of traceability of transactions, identification of users (through the authentication and identification operated by exchangers) could help detect and disrupt TF-related abuses.

[131] In the sample group of hawaladars interviewed for the purposes of the UNODC 2023 report, twenty-two participants said they did not use digital currencies. Only five of the study participants (based in Bosnia and Herzegovina, Austria, Nigeria, and Romania) reported using cryptocurrencies including Bitcoin, Ethereum, and Tether (USDT). However, fifteen hawaladars – based in the United Republic of Tanzania (4), Romania (1), Kazakhstan (4), Afghanistan (3), Spain (2), and Austria (1) – mentioned they were aware of other hawaladars who used crypto currency. *See* UNODC, The Hawala System: Its operations and misuse by opiate traffickers and migrant smugglers, 2023—available at www.unodc.org.

[132] Valeri M., Fondacaro R., De Angelis C., Barella A., European Journal of Islamic Finance, The Use of Cryptocurrencies for Hawala in the Islamic Finance—available at www.ojs.unito.it

© FATF-OECD 2025

Case study: ISIL facilitators using a variety of MVTS, including HOSSP

ISIL facilitators in South Africa have emerged as critical intermediaries in the collection, movement, and consolidation of funds across the African continent. After pooling money in South Africa, ISIL operatives help distribute it across East Africa, including to DRC, Uganda, Tanzania, and Mozambique. Key financial mechanisms employed include the hawala system, remittance service providers, and exploitation of formal FIs.

For instance, between 2019 and late 2020, a Johannesburg-registered company with operations in Mogadishu, helped facilitate the movement of nearly USD 400,000 across Somalia, South Africa and other East African countries.

These transfers were conducted via regional hawala and remittance networks—including Taaj, Juba Express, and Mama Money—some of which maintain branches across East Africa, the Middle East, and Western jurisdictions. Facilitators used third-party intermediaries, MVTS providers, and virtual vaults—such as Selpal, Flash, and Kazang—to obscure transactions from the formal banking sector. The company also utilized legitimate bank accounts to conceal and transfer balances.

In September 2021, authorities dismantled the company's network. Subsequent measures included the creation of a dedicated private sector reporting hotline for illicit domestic and cross-border MVTS activity, as well as the strengthening of public-private partnerships (PPPs). These efforts were supported by the South African Anti-Money Laundering Integrated Task Force, through its Expert Working Groups and Tactical Operational Groups.

Source: South Africa

Note: Based on the above, South Africa designated two individuals and two entities under its domestic designation framework established pursuant to UNSCR 1373 (2001). See: Media Release and Notification (12 February 2025).

3. Methods based on e-money

3.1. Mobile money

151. Mobile money is the provision of financial services through a mobile device[133]. Mobile money products are often linked to prepaid accounts and/or non-banking FIs[134]. Mobile money products often operate under different AML/CFT requirements than

[133] World Bank Chapter 4: Mobile Money for Financial Inclusion, Kevin Donovan (2012)

[134] In that stage, given that mobile money products are often linked to prepaid accounts, non-banking entities also have been very active. In fact, telecommunications providers have been successful mobile money issuers. During this stage, several jurisdictions have been confronted with these developments and have either allowed their development without specific regulation, regulated them with special licensing or registration requirements, or forbidden their operation. However, in emerging markets forms of mobile money, including mobile payments, are growing and contributing to financial inclusion as these provide under-served and unbanked people with access to a broad range of formal financial services.

© FATF-OECD 2025

traditional banks. In addition, these products typically integrate tiered Know Your Customer (KYC) in their frameworks. FIs that facilitate mobile payments, including person-to-business, person-to-person or government-to-person transactions can be traditional service providers (bank or depository institutions) and/or MVTS[135].

152. Terrorist organisations have increasingly leveraged mobile money platforms to solicit donations, collect funds from supporters, and move money between operatives. Mobile money gained increased significance for terrorists, especially in jurisdictions where registration of SIM cards is not strictly enforced and where mobile money operators are not subject to AML/CFT regulations and lack awareness of the terrorism-financing risks[136]. The risk is amplified in regions where mobile money services integrate seamlessly with banking services, particularly in regions with limited banking infrastructure. In sub-Saharan Africa, mobile money platforms are linked to informal money transfer networks, such as hawala, which enable cross-border transfers without oversight. In such context, mobile money is often used to transfer funds to terrorist fighters as final beneficiaries: funds collected by financial managers, especially in regional financial hubs, are distributed to various branches regionally, until the stage when funding is split in small amounts to be sent to fighters conducting operations.

153. In conflict environments in Africa, such as Somalia, DRC, and in Mozambique, comprehensive CDD requirements may not be properly enforced as the displaced populations fleeing conflict may not have their identification documents. Hence, terrorist groups operating in the refugee and displacement camps can easily take advantage of the conflict situation to transfer funds across borders through mobile money with minimal scrutiny[137]. Conflict also provides an enabling environment for terrorist groups to benefit from criminal activities (including KFR, receiving donations from sympathisers, extortion or payment for supplies and logistics for terrorist purposes) which can be facilitated through mobile money channels. Indeed, the abuse of mobile money services in Somalia exemplifies terrorist activities financed through organised crime. Groups like Al-Shabaab[138] use strategies such as frequently changing mobile-phone numbers to evade detection. Their finance officers often maintain mobile money accounts with a limit of as much as USD 100,000[139], and collect extortion payments in the form of hawala "taxes" through multiple accounts registered under false identities.

154. According to INTERPOL, the emergence of mobile e-money platforms like M-Pesa in East Africa has enabled terrorist organisations to misuse these and exploit them to circumvent traditional banking methods. This is notably evident with Al-Shabaab[140], which

[135] FATF Guidance for a Risk-Based Approach on Prepaid Cards, Mobile Payments and Internet-based Payment Services

[136] For example, see GABAC Republic of Chad Mutual Evaluation Report (2023), page 87.

[137] Kenyan authorities have maintained that several terrorist attacks conducted by Al-Shabaab in the country are planned in the Dadaab Refugee camp.

[138] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[139] Somalia Monitoring Group, S/2018/1002.

[140] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

depends on mobile money for transferring resources to its operatives and for logistical needs, particularly in areas where formal financial services are scarce. One attacker of a Kenyan hotel in January 2019 had over thirty SIM cards in use according to the Kenyan authorities[141], which demonstrates the vulnerability of mobile money usage as a TF method. The UN has also noted the use of mobile money by ADF[142] to support its activities in prisons where mobile money transfers from ADF leadership are received and redistributed for recruitment, sustenance of detained fighters and mobilisation of other inmates[143].

155. In West and Central Africa, the use of mobile money methods for terrorism is less common, but still present. AQIM operatives were arrested with several SIM cards and cash, maintaining communication with other terror networks, which demonstrates the potential for mobile money exploitation[144].

156. Ultimately, mobile money services have become crucial tools for TF across various regions. This exploitation is enabled by factors such as lax SIM card registration, weak AML/CFT regulations, integration with banking services, and connections to informal networks like hawala, requiring robust measures to prevent financial activities that fuel terrorism.

Case study: Mobile money transfers within a terrorist organisation

In 2023, the Uganda High Court—International Crimes Division (ICD) convicted four individuals for affiliations with the designated terrorist group ADF[145], TF, and aggravated trafficking in persons and children. The four suspects were sentenced to seven imprisonment years.

Between May 2018 and July 2019, under direct orders from ADF leaders, the group recruited new members and facilitated their transport from Uganda to ADF camps in the Democratic Republic of Congo (DRC). Investigations revealed that mobile money transfers were used to finance these activities, covering logistics, maintenance, and the purchase of improvised explosive devices (IEDs). The recruits were transported by bus from Uganda's eastern regions—Mayuge and Mbale Districts—via Kasese District, which borders DRC, an area with an active

[141] The Standard Newspaper, How Dusit attacker communicated, moved money – DPP Haji, by Betty Njeru (2022).

[142] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[143] Group of Experts on DRC, S/2024/432

[144] FATF, GABAC and GIABA joint report on Terrorist Financing West Central Africa (2016)

[145] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States. This applies for all references to ADF in the text box.

© FATF-OECD 2025

ADF presence. The suspects knew the recruits would be used to carry out or support acts of terrorism on behalf of ADF.

Source: Office of the Directorate of Public Prosecutions, Uganda.

3.2. Online payment services

157. One significant market development in recent years has been the emergence of a wide array of payment service providers (PSPs), including digital ones—commonly referred to as FinTech companies. While there is no FATF definition or generally accepted industry definition of PSPs, this sector is understood to encompass entities that provide funds transfers, including credit transfers, payment to merchant instant payments, direct debit, money remittances whether domestic or cross-border, as well as transfers carried out using a payment card, an electronic money instrument, mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.

158. The PSP sector is constituted by multiples actors working together to enable the digital payment ecosystems. The PSP sector is a highly diverse sector, ranging from traditional brick and mortar banks, neobanks, to card processors, to online or mobile solutions that facilitate payments. Generally, the banks providing payment services are well-known and have been subject to significant AML/CFT/CPF regulation and risk-based supervision for decades. The non-bank sub-sector of the PSP[146] sector features more new entrants and those that have, in some cases, sat outside of the AML/CFT/CPF regulatory regime. The non-bank sub-sector does include some household names but also providers that consumers may not be able to readily identify despite using their services[147].

159. Many PSPs in the non-bank sector often offer their services leveraging online through Fintech technology platforms. FinTech's companies can be acting as third party that provide services, assisting merchants with the acceptance of digital payments by, for example, communicating with the customer's bank or card issuer to verify transaction details, check for sufficient funds, and obtain authorisation. New financial technologies have helped with enabling the acceptance of more payment methods in a secure manner, including purchased payments, P2P payments, micropayments and donations, crowdfunding, digital wallets, buy-now-pay-later, e-commerce, and subscriptions.

160. As the offer of online payment services from Fintech companies has grown substantially over the last ten years, cases of terrorists opting for those services can be observed across all contexts, especially as it offers an opportunity to diversify fund-moving channels. These payment services also appear attractive for terrorist organisations for the low-cost and fast money transfer solutions they offer, with possibility for enhanced opacity on initiators and beneficiaries through pseudonyms or fake accounts.

[146] FATF confidential report (FATF/RTMG(2025)17): Non-banks represent a very diverse range of entities that have increased competition in the payments market that are disrupting the market through technological advancements. The business models of non-bank PSPs, in some cases, offer substitutions to bank offerings, while they complement bank offerings in others. This breaks down of traditional services into more specialised components, unbundles traditional payment chains. The greater inclusion of non-bank PSPs into the market has led to more players being involved in payments, complexifying the market, and segmenting it from its historical concentration in banks.

[147] FATF confidential report (FATF/RTMG(2025)17).

© FATF-OECD 2025

161. Europol assesses that services are commonly used across all types of terrorist organisations. In cases involving small terrorist cells, FTFs, and other individual terrorists, P2P payment services have been used for procurement of military equipment, chemical components, or propaganda materials on e-commerce platforms (EPOMs). Delegations also report that EoRMT groups use peer-to-peer payment systems to sell merchandising, items conveying extremist ideologies (books, music, clothes) to sympathisers, which constitutes a central source of revenue for those organisations.

162. Such online payment services can also be used to convey donations to larger organisations, especially in the extent that some payment mechanisms are directly integrated into social networks and content hosting services. In those cases, a single platform can be used to recruit donators, launch a crowdfunding campaign, and proceed to the transfer of funds through an online payment service. As it was mentioned regarding credit cards, online payment services offer less traceability and transparency compared to wire-transfer, making it harder to clearly identify initiators and recipients of transfers.

Case study: Use of online payment service and VPNs to fund lone actor terrorist act

On 3 April 2022, individual A attacked security personnel at Gorakhnath Temple, influenced by ISIL's ideology. The attack was detected during the breach attempt, leading to immediate arrest. The case was transferred to Uttar Pradesh ATS, who uncovered ISIL influence through forensic analysis of individual A's cell phone.

The financial investigation revealed that individual A transferred INR 669,841 (USD 7,685) via PayPal to foreign countries in support of ISIL, using international third-party transactions and using VPN services to obscure the IP address. He also received INR 10,323.35 (USD 188) from a foreign source.

Investigations evidenced foreign financial transactions supporting ISIL activities. The detection of deposits and transactions was facilitated through a multi-tiered investigative approach. Initially, the local police conducted a preliminary inquiry, which was subsequently taken over by the Anti-Terrorism Squad (ATS). The ATS meticulously examined the evidence collected, including the accused's phone, which was sent for forensic analysis. The forensic report revealed that the accused had been using a VPN for calling, chatting, and downloading to evade detection. Further financial scrutiny uncovered that the accused had made a payment to a VPN provider through his bank account to secure these services. A comprehensive analysis of the accused's PayPal transactions, obtained via email, indicated that approximately forty-four international third-party transactions totaling Rs. 669,841 (approximately USD 7,736) had been made to foreign accounts. Additionally, the accused received funds from a foreign account through PayPal. The investigation also uncovered that the accused had sent money to multiple individuals identified as ISIL followers in in foreign jurisdictions to support terrorist activities. Due to the suspicious nature of these transactions and the potential for TF, PayPal suspended the accused's account, thereby preventing further illicit fund transfers.

Source: Ministry of Finance, India

© FATF-OECD 2025

4. Methods based on the abuse of traditional financial services

163. Traditional financial services are still used by terrorist groups for their financing activities, even though they seem to appear less frequently in TF cases compared to schemes involving underground and anonymous operations through cash, collectors, or hawala network. Despite the evolution of international standards on beneficial ownership and transparency, and the improvement of identity verification systems, terrorist organisations continue to rely to some extent on formal financial services to move and store funds, by targeting jurisdictions with weak CFT enforcement and insufficient or restricted international cooperation mechanisms. In other contexts, it seems that proper implementation of AML/CFT measures resulted in terrorist organisations and individuals increasingly avoiding the financial sector.

164. As a general observation, preventing or detecting the abuse of formal financial services for terrorist purposes is particularly challenging when it relates to non-designated groups and individuals, or when designations are not recognised in all jurisdictions involved in a cross-border financial operation. For example, this challenge has been referred in relation to EoRMT groups and individuals as their designations (and lack thereof) appear to be particularly inconsistent among jurisdictions.

4.1. Banking services

165. Mainstream banking services covered in this section are deposit accounts, wire-transfers, credit cards, credit loans, and online or mobile-banking services.

166. Terrorist groups with transnational activities are occasionally reported as using banking deposit accounts. Those bank accounts can be used as storage mechanism, even though it appears significantly less common than cash reserves. When this does occur, accounts are likely to be opened in the name of third parties or front companies, or held in different jurisdictions, to disguise beneficial owners' identities. Some delegations also report that bank accounts are more likely to be used in territories under terrorist organisations' control. Mozambique reported that there is evidence of legal and natural persons receiving money through bank transfers and of large sums being withdrawn in areas of Cabo Delgado affected by terrorist acts without plausible justification. Deposit accounts are also commonly observed in cases involving small terrorist cells or individual terrorists avoiding detection, especially as they tend to operate with low amounts generated from legal sources.

167. Wire-transfers can still be observed for transnational movements of funds aiming at financing terrorism, although this method appears as much rarer than hawala, cash transportation, or MVTS. Jurisdictions report wire-transfers in cases involving transnational terrorist organisations, as well as groups active at national or subnational level but affiliated to larger terrorist networks. In Australia's experience, such transnational transfers mostly consist of small and medium amounts (less than USD 10,000 typically), usually in one or two transactions. Türkiye reports on wire-transfers operated by Turkish nationals or foreigners towards ISIL, with transaction descriptions including explanations such as "infaq, zakat, fitra, charity, prison camp, for captive sisters, for Syria". TF-related bank transfers can also be observed within national borders, among members or sympathisers of terrorist groups operating in restricted geographies. Thailand reports that such transfers mostly consist of small amounts and are thus difficult to detect but can be identified through investigations and suspicious transaction reports.

© FATF-OECD 2025

168. Credit and debit cards are also still used in TF cases, especially involving small cells or individual terrorists. EU-based AQ sympathisers were reported using credit cards linked to bank accounts located outside the European Union to purchase VAs aimed for donation to the terrorist organisation. Singapore also observed credit cards used by self-radicalised individuals to transfer funds internationally. Compared to wire-transfers, credit cards can in some configurations offer less traceability and transparency on identities of both the initiator and recipient (for instance when the transaction is disguised as a commercial payment). Credit cards can be used by terrorists to cover individuals' expenditures, especially when funds were generated from licit sources (salaries, social benefits, family support), or when bank accounts of legal entities (companies, NPOs) are used as a front.

169. Cases were also reported involving the abuse of fraudulently obtained credit cards acquired abroad through forged documentation schemes. These cards were used to purchase goods—such as mobile phones and other technological devices—either distributed to individuals supporting operational activities or sold to finance terrorism-related purposes, including document procurement, residency regularisation for terrorist actors, and recruitment efforts.

Case study: Use of credit cards and e-money accounts and payments to facilitate TF in Luxembourg

The case was detected based on international cooperation between law enforcement authorities (LEAs) regarding a Luxembourgish citizen spreading ISIS-related content on social media. The suspect focused on the pseudo-religious legitimisation of the ISIS ideology and managed to circumvent the measures taken by social media platforms prohibiting such content. The suspect radicalised after the departure of his close friend as a FTF in the Syria/Iraq area.

First results showed that the suspect was holding a bank account and an associated debit card within a bank in Luxembourg, as well as an active account with a payment and e-money institution. Further analyses revealed that the credit card associated to the identified payment and e-money account was also connected to two further payments and e-money accounts held by two unknown individuals. In addition, a total of four payments and e-money accounts seemed to be linked between each other by either the physical address, e-mail addresses or IP addresses. The observed account movements were mainly purchases of religious clothing for Muslim women, transfers to marriage agencies or donations to religious NPOs.

In addition, suspicions were raised that the suspect's wife was involved in the case too. An exhaustive transactional analysis was performed on her payment and e-money accounts and suspicious transfers were identified as to an individual who matched a suspect in the FIU's databases. The individual was suspected in a bordering country to have links to TF.

Red flag indicators included frequent transfers and donations made to religious NPOs with ties to extremist movements, but also to NPOs with the intent of

© FATF-OECD 2025

financially support widows, families of deceased fighters and prisoners in conflict areas and high-risk jurisdictions in terms of terrorism and TF risks.

Source: Luxembourg

170. Regulated banking services intervene in a larger extent in financial management of small cells and individual terrorists, as well as EoRMT groups, even though they have occasionally been reported in cases involving larger organisations.

171. Deposit accounts are more likely to be used for storage purposes in contexts involving low-scale endogenous threats and entities or individuals engaged in EoRMT. This is due to the relatively limited amounts of funds involved and the fact that such funds are often derived from legitimate sources, such as salaries, social benefits, or financial support from relatives. These characteristics enable such individuals to operate below the detection thresholds of financial monitoring systems. Delegations reported that funds from saving accounts are typically withdrawn by self-radicalised individuals and FTFs to be spent in cash.

172. Also, as pointed out in Section 1, regular credit loans have been used by FTFs to fund their departure to theatres of operations, or by individuals to conduct local attacks outside conflict areas. Some of those loans have been contracted using document fraud. Terrorists can also use their relatives or friends to contract the loan in their own name to hide the true beneficiary.

173. According to Australia, major banks are more likely to be exposed to TF risks given the size of their customer base, scale of operations, cash transaction infrastructure, and global reach. They are also the key conduit for international transactions in and out and serve as correspondent banks for other FIs. Still, several delegations called for greater attention to be paid to the TF abuse and vulnerabilities of new banking actors, including "neobanks", mainly referring to banking institutions operating exclusively online. These banks are drawing a growing number of customers and are increasingly mentioned in cases of TF. The fact that many neobanks are still emerging actors in process of strengthening their internal compliance procedures, combined with the remote nature of their activity, can result in weaker CDD capacity and more discretion compared to more traditional credit institutions. Other innovative financial instruments, such as virtual IBAN, are drawing increasing attention from jurisdictions in terms of TF risks, as they provide new opportunities to obfuscate the final destination and beneficial owners of wire transfers.

© FATF-OECD 2025

Case study: Deposits on shell bank accounts and immediate withdrawal of cash to finance a terrorist act

In 2021, a vehicle-borne improvised explosive device exploded in a large city in Pakistan resulting in several casualties. The attack was claimed as being executed on behalf of the Tehrik-e Taliban Pakistan (TTP). The Counter Terrorism Department (CTD) started a terrorist investigation and revealed that Person A was the key suspect, and the owner of the vehicle used in the attack. A joint investigation team was also set up to conduct a parallel financial investigation under the Anti-Terrorism Act (1997) which included TF offenses.

The financial investigation showed that Person A, a resident of the biggest city of Pakistan, visited another large city of Pakistan where he reactivated a dormant bank account, conducted a cash withdrawal transaction—9,400 Rs (approximately USD 109) from one bank account, and two transactions of PKR 20,000 (approximately USD 72) —and then closed the accounts. The withdrawn funds were then allegedly used to purchase the vehicle which was used in the terrorist act. Person C provided logistics to Person A, which is also a brother of a designated person. Person C was later identified as key suspect in the attack. The detailed analysis found that the financier of Person A and D had two type of financial transactions that linked them:

Person D gave PKR 1,000,000 (approximately USD 3590) to Person A in cash and made two transactions of PKR 20,000 each with Person A through his account, apparently for TF purposes. Further investigation by CTD led to identify Person A's financier as the mastermind behind the terror attack. The Financial Monitoring Unit (FMU) identified that Person A had received two remittances—PKR 150,000 (approximately USD 540) and PKR 100,000 (approximately USD 360) respectively—from a foreign jurisdiction. FMU established that Person A was frequently travelling to foreign jurisdictions where the mastermind, facilitators, and sponsors were residing.

The mastermind/financer, executor, and facilitators were arrested and subsequently convicted.

Source: National Counter Terrorism Authority (NACTA), Pakistan.

4.2. Prepaid cards

174. Prepaid cards are cards with data encoded directly in the card, or stored remotely, that are pre-loaded with a fixed amount of electronic currency or value. They can allow easy transfer of value are often used as an alternative to traditional bank accounts and credit cards. While there are a wide variety of prepaid cards, the category of card of most concern is open-loop cards where funds can be withdrawn at Automatic Teller Machines (ATMs) worldwide[148]. These are network-branded payment cards that allow transactions with any merchant or service provider participating in the payment network (e.g., Visa or

[148] FATF Guidance for Risk Based-Approach on Prepaid Cards, Mobile Payments and Internet-based Payment Services (2013)

© FATF-OECD 2025

MasterCard). General Purpose Reload (GPRs) cards are financial products that consumers can apply for online or pick-up from the prepaid section at various retailers. These cards are activated later by the consumer by phone or online. These products function like any other bank-issued debit card but offer greater anonymity for they can be reloaded through coupons purchased by cash.

175. One vulnerability of prepaid cards is that there can be ambiguity regarding the legal status of this financial service and a lack of uniformity in regulation across jurisdictions, which makes them attractive for TF abuse.

176. Prepaid cards share similar vulnerabilities to those presented regarding mobile money and HOSSPs. This is due to their potential for anonymity and ease of cross-border transfers. Prepaid cards are easily transportable and tradeable: they can be purchased in one location and used in another, making it difficult to trace the movement of funds. Prepaid cards are not always as strictly regulated as other forms of financial services and can be distributed by diverse actors with unequal due diligence processes. This can make prepaid cards an easier way to circumvent traditional banking controls, including by using stolen identities to procure prepaid cards which can then be shipped to other jurisdictions without detection.

177. Prepaid cards have been used by terrorists, and FTFs in particular, to store and move funds internationally. Generally, the cardholder can be located in conflict area, while an accomplice can proceed to buy reloading coupons in cash or VAs in another jurisdiction, to then share the reloading code with the bearer for him to be able to withdraw cash through ATMs. Italy also reports that while MVTS are the most common method for terrorist organisations to move funds internationally, prepaid cards are the most exposed vector for domestic movement of funds for terrorism purpose as cards are bought by third parties that go through CDD processes and registration, before handing cards back to members of an organisation, who will share top-up codes and use IBANs associated with cards to exchange funds internally[149].

178. Besides fund-moving purposes, prepaid cards can also be used by self-radicalised individuals to purchase propaganda products in a less traceable way.

179. However, the use of prepaid cards does not provide significant advantages for members of terrorist organisations when, similarly to banking services, they require some formalities and documentation processes to obtain and maintain them. In many jurisdictions, prepaid cards are offered as a financial service, and thus embedded with the formal banking system. In such case, it would require one to first operate bank accounts, subject to due-diligence or KYC policies, before being issued with prepaid cards. Many prepaid cards require monthly maintenance fees, activation fees, and fees chargeable per transactions which makes it a costly choice for TF. Additionally, they have ATM withdrawal limits which makes it restrictive for use by terrorist organisations.

180. Overall, the use of prepaid cards is prevalent in regions with high banking penetration, which can allow the prepaid cards, especially the open loop cards, to be used to withdraw cash from ATMs or to make purchases that support operational needs.

[149] See also FATF Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling (2022), case study 7, pages 28-29.

© FATF-OECD 2025

5. Methods based on the abuse of digital platforms

181. Jurisdictions report increased use of digital platforms, including social media, content hosting and direct messaging services, online merchandise sales, crowdfunding, and mobile communication applications, among others, by various terrorist groups across the ideological and geographical spectrums, as well as by individual terrorists, including FTFs. Various VAs exchanges, stablecoins, and e-wallets have been used to raise and transfer or store terrorist funds. As the abuse of digital platforms for TF purposes is expected to become more pervasive and significant[150], recent trends underscore the need to enhance the understanding of the TF risks associated with new and emerging financial technologies and fundraising methods as the first and critical step for developing appropriate response[151].

182. Many of these digital technologies are used in various combinations depending on circumstances and targeted goals and are mutually supportive or complementary. Often, online fundraising campaigns overtly advertised through social media and Internet sites are framed under disguised appeals for humanitarian relief or other charitable causes. The use of Quick Response (QR) codes[152] by various types of terrorist groups has been on the increase both for announcing certain events and to solicit donations or communicate wallet addresses. Encrypted communication applications are popular for facilitating fundraising by terrorists as they allow unguarded discussions regarding payment methods and actual intended use of funds. There are also other fundraising opportunities that can be facilitated by online technologies and abused for terrorist purposes, such as the super chat feature or brands advertising and offering monetisation alongside terrorist content, as trends and tactics continue to evolve[153]. Some jurisdictions report that the "dark web" has become a hub for TF allowing terrorists to sell and purchase weapons, drugs, stolen data as well as raise and launder money under anonymity.

183. Even though the increase in use of these methods has been observed with most categories of terrorist groups and individuals, the scale and types of abuses vary depending on regional and economic context, available means, and the targets set by terrorists in terms of their financing sources and methods[154]. Research indicates, for example, that VAs may have limited functionality for the so-called "lone actor" or "self-activating terrorists", who can easily acquire the modest funds needed to finance their

[150] United Nations, thirty-fourth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning Islamic State in Iraq and the Levant (ISIL), Al-Qaida and associated individuals, groups, undertakings, and entities (S/2024/556), paragraph 95

[151] UNSC Counter-Terrorism Committee, Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 17.

[152] QR codes are an access method that simplify sending funds by removing the need to manually insert account details. They have been a major driver in the accessibility of digital payments.

[153] UNSC Counter-Terrorism Committee, Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 10.

[154] UNSC Counter-Terrorism Committee, Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 9.

© FATF-OECD 2025

attacks through everyday means[155]. These technologies may be less useful so long as precursor chemicals for explosives or edged weapons can be procured in shops or online marketplaces using regular payment methods.

184. In general, FTFs, have also increased their use of mobile money, VAs, social media, mobile applications, and instant messaging services[156]. An additional trend has emerged of funds being raised online, often in VAs, to sustain or smuggle ISIL-related FTFs and/or their family members detained in camps and prisons[157].

185. With respect to fundraising for terrorist groups to cover organisational costs, technologies such as social media, VAs and crowdfunding, are more often used in combination with more traditional TF methodologies. Furthermore, while fundraising online campaigns with use of VA were initially very explicit and shared in open social media, they have since moved to more private environments and are often disguised under seemingly legitimate causes. This is at least in part due to the rising awareness that some VA transactions are successfully traceable and detectable, and VASPs are increasingly subject to AML/CFT regulation and supervision.

186. Many of the digital methods discussed in this Section are widely accessible, low-cost and can reach global audience. For example, fundraising campaigns with the use of digital / online platforms can be established quickly with varying degrees of identity verification requirements and be dissolved equally as fast to avoid disruption. Overall, the technologies most abused for TF are rarely the most sophisticated innovations, but those with the greatest uptake in society overall. And risks tend to shift over time in the same manner: as digital platforms and methods become more available, prevalent, and mainstream with wider public use, the frequency of their abuse for TF purposes has increased.

[155] RUSI, Occasional paper on Bit by Bit. Impacts of New Technology on Terrorism Financing Risks, Stephen Reimer and Matthew Redhead (2022)
[155] UN CTED 2024 Trends Tracker.
[156] UN CTED 2024 Trends Tracker.
[157] See Section 1.

© FATF-OECD 2025

Case study: Donation through online fundraising campaigns supporting Syria-based terrorist organisations

Singapore's security agency identified a potential TF activity and referred the case over to the Commercial Affairs Department of the Singapore Police Force—the country's lead agency for CFT investigations and enforcement. The TF investigation revealed that, on 15 occasions in 2020, an individual (Person B) allegedly transferred sums amounting to up to SGD 891 (approximately USD 660) via online platforms to fundraising campaigns intended to support Hayat Tahrir al-Sham (HTS). Upon the conclusion of their TF investigations, the Commercial Affairs Department recommended that Person B be prosecuted for TF offences under the Terrorism (Suppression of Financing) Act 2002, Singapore's CFT legislation.

Person B was aware that the funds, either wholly or in part, would benefit HTS's activities, having been radicalised and having expressed ideological alignment with the group. He was subsequently convicted of providing financial support for terrorist purposes and sentenced to two years and eight months' imprisonment. Following the completion of his sentence, Person B was repatriated to Country Z. Person B continues to be listed on the First Schedule of the Terrorism (Suppression of Financing) Act 2002, Singapore's domestic terrorist designation list established pursuant to UNSCR 1373 (2001).

Source: Ministry of Home Affairs, Singapore.

5.1. Social media and messaging services

187. The FATF has already highlighted the use of social media for TF purposes in its 2015 report. Over the past decade, social media and messaging services technologies have dramatically evolved, changing our communication systems and infrastructures, multiplying channels of communication, and fostering anonymity and outreach to massive audiences across borders. However, these communication systems come with vulnerabilities that are abused by terrorist organisations and individual terrorists or supporters to further decentralise, spread their terrorist propaganda, reach out to global sympathisers, and raise funds in various forms, including fiat currency, prepaid cards, and VAs. Social networking services (SNS), content hosting services, crowdfunding services and Internet Communication Services have been abused in a variety of ways for TF[158].

188. In general, SNS are primarily misused to promote terrorism through propaganda and radicalisation-content, and to solicit donations. Content hosting services are used in many cases to privately communicate with campaigners or terrorist groups and discuss means of support and payment methods. Some of these services have also integrated

[158] UNSC Counter-Terrorism Committee, Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 10—available at https://docs.un.org/S/2025/22; S/2024/556, paragraph 94; APG and MENAFATF joint report on Social Media & Terrorism Financing Report (2019)

© FATF-OECD 2025

traditional and new payment services. Some platforms allow in-app gifting, "tipping" or live-stream donation features, which can be converted into cash or VAs.

189. Social networks are widely coupled with formal and informal crowdfunding platforms or features[159]. Funds collected through such means can be moved through formal banking channels and other registered payment services, or with the use of online remittance services and alternative banking systems that do not enforce rigorous AML/CFT measures. In some cases, larger transactions are split into multiple smaller ones and routed through intermediaries to avoid detection.

190. Various terrorist organisations, including territory-controlling and large networked organisations, have been reported to disguise fundraising for terrorism as humanitarian and/or charitable campaigns on social media platforms, by collecting small donations from sympathisers worldwide. These campaigns are generally linked to bank accounts, mobile payment services and digital wallets, that can operate with VAs. When the accounts are blocked, organisers quickly advertise new accounts or wallets through the same platforms, ensuring fundraising continuity. These mechanisms, coupled with the relative ease with which they integrate electronic payment services, make the abuse of social media and instant encrypted messaging applications a convenient vector to generate significant revenue in minimal time and limited traceability. Occasionally, this method is coupled with the abuse of NPOs where purported charitable fundraisers divert funds from charitable or humanitarian campaigns to the benefit of terrorist-related accounts. Overall, informal fundraising campaigns are adaptive to disruption measures and tend to move to closed social media and applications groups for communication.

191. Large-scale and well-organised fundraising schemes aimed at TF may involve up to several thousand 'sponsors' and may raise significant amounts of funds through donations. Terrorist organisations reach out to large audiences through P2P horizontal communications, chats, forums and/or group channels hosted on social media (such as Facebook, Instagram, X, TikTok, among others). In addition, new technologies, such as live streaming video platforms, further enable these organisations to call for donations while carrying out propaganda campaigns. Additionally, social media algorithms, which are powered by artificial intelligence (AI), direct users to specific content based on their preferences and browsing habits. In the context of terrorist propaganda and radicalisation-content, these algorithms may expose at-risk users to content or networks that reinforce extremist beliefs, potentially identifying prospective donors and directing them to targeted campaigns.

192. The involvement of social media platforms in fundraising campaigns for TF purposes creates challenges for operational authorities in terms of engagement and cooperation and raises questions regarding what responsibility lies, or should lie, with these actors. Despite repeated instances of the use of social media and crowdfunding platforms by terrorists for financial activities, some platforms or chat applications face challenges in adapting self-monitoring and content moderation systems to address TF that may be occurring through their platforms[160]. Yet, social media and other non-financial sites have a vital role in monitoring fundraising patterns and financial communication, i.e.,

[159] See sub-section 4.2.

[160] UNSC Counter-Terrorism Committee, Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 10 noting, for example, that under the European Union Digital Services Act, large platforms are required to conduct their own risk assessment and remove illegal content upon notification from authorities, but there is no explicit reference to terrorist financing as a form of illegal content.

© FATF-OECD 2025

knowing their users, whereas payment service providers have the necessary information to know their networks.

193. Terrorist organisations and individuals are reported to increasingly use instant and encrypted messaging applications (such as WhatsApp, Telegram, Viber, Signal and others), including private chats that guarantee the anonymity of the users, as well as secure networks like Surespo and VoIP. Terrorists use these services to share financial data (including IBANs, wallet addresses or other means of payment), campaign details, and donation instructions (included coded language) while avoiding detection. Features such as "self-destruct" messages, which erase after a set time, further complicate tracking efforts. Social media and encrypted communication applications may allow unguarded conversations regarding payment methods and actual intended use of funds.

© FATF-OECD 2025

Case study: Misuse of MVTS and self-exposure on social media to support a terrorist organisation in the United States

In 2020, in the District of New Jersey, United States, a person ("Xie") plead guilty to one count of concealing attempts to provide material support to a designated foreign terrorist organisation ("FTO").

According to documents filed in this case and statements made in court, Xie admitted that he knowingly concealed and disguised the nature, location, source, ownership and control of the attempt to provide material support and resources to Harakat al-Muqawamah al-Islamiyya and the Islamic Resistance Movement, an organisation that is commonly referred to as Hamas[161]. Xie admitted that he knew Hamas was a designated FTO in the United States and has engaged in terrorist activities. He said he attempted to conceal the attempted support believing it would be used to commit or assist in the commission of a violent act.

In December 2018, Xie sent USD 100 via Moneygram to an individual in the Gaza Strip who Xie believed to be a member of the Al-Qassam Brigades—a faction of Hamas that has conducted attacks. At approximately the same time that Xie sent the money, he posted on his Instagram account *"Just donated USD 100 to Hamas. Pretty sure it was illegal, but I don't give a damn*". In April 2019, Xie continued his appearance in social media (Instagram Live video) wearing a black ski mask and stated that he was against Zionisim and the neo-liberalism establishment, that he would join the organisation and after displaying the organisation's flag and a handgun, he expressed his intention to commit a violent act.

Also in April 2019, Xie sent a link to a website for the Al-Qassam Brigades[162] to an FBI employee who was acting online in an undercover capacity and described the website as owned by the organisation. He mentioned he had already used the website to donate funds and demonstrated to the FBI employee how to use a new feature on the website that allows anonymous donations to be sent via VAs (Bitcoin).

The investigation revealed additional social media accounts for Xie, including a YouTube account which contained, among other things, a playlist containing videos, many of which advocated or propagandised Soldiers for Allah, the war in Syria, Hezbollah[163] (also a designated FTO to the United States), and the Houthi

[161] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). This applies for all references to Hamas in the text box.

[162] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[163] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

© FATF-OECD 2025

movement[164] in Yemen, as well as support for Bashar al Assad, Saddam Hussein, and North Korea.

Source: Department of Treasury, United States [District of New Jersey | Somerset County Man Sentenced to 64 Months' Incarceration for Concealing Material Support to Hamas | United States Department of Justice]
Note: This case study references organisations listed under a domestic designations sanction list [Foreign Terrorist Organizations - United States Department of State].

Monetisation and other income-generating features on social media platforms

194. While economic models of social networks remain primarily based on targeted advertising aimed at users, some increasingly rely on commissions collected from integrated payment systems and internal transactions instruments. These advancements reflect a broader trend toward diversifying monetisation options on social media, providing creators with multiple streams of income and fostering deeper engagement with their audiences.

195. Monetisation strategies on social media platforms have evolved significantly, offering creators diverse avenues to generate income and engage with their audiences. Key developments include:

- Super Chat Feature: YouTube's Super Chat allows viewers to purchase highlighted messages during live streams, enhancing their visibility and enabling direct interaction with creators. These messages can remain pinned for up to five hours, depending on the contribution amount, providing fans with a way to support creators financially while gaining recognition.
- Subscription-based models are gaining traction. Platforms like Patreon and OnlyFans allow creators to offer exclusive content to subscribers for a fee. This model provides a steady revenue stream for creators and allows fans to support their favourite content producers directly. A premium subscription on X platform provides, along with the checkmarks which are intended to confer legitimacy, a variety of perks, including the ability to post longer text and videos and greater visibility for some posts.
- The tipping function on X, now called "Tips" allows users to tip other accounts using various payment methods, including VAs. To use Tips, the recipient must have enabled the feature and linked their account to third-party payment processors. A recent research found blue check-marked accounts related to sanctioned groups or individuals using this feature[165].
- Virtual events and live streaming have become popular monetisation strategies. Platforms like Zoom and YouTube Live enable businesses and creators to host events that can be attended by a global audience. These events can be monetised through ticket sales, sponsorships, and donations from viewers.

[164] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).
[165] Tech Transparency Project, "US-Sanctioned Terrorists Enjoy Premium Boost on X", 15 May 2025—available at www.techtransparencyproject.org.

© FATF-OECD 2025

- Rewarded ads are becoming more popular to engage users. These ads offer users rewards, such as in-app currency or premium content, in exchange for watching ads.

196. Integrated payment features for internal transfers can pose a challenge in terms of traceability: when funds enter the inhouse payment system, AML-CFT obliged entities have limited visibility regarding the ultimate destination. Then, when transactions take place within the platform, only the social media have visibility over those. Finally, when funds leave the internal platform, financial labels associated with the credit flow can give information on the social platform it is coming from but can also sometimes only display information on financial intermediaries, which means the origin of funds is obstructed.

Case study: Conversion of social network's 'virtual currency' into VAs to finance terrorism

In 2024, an influencer promoted donation campaigns launched on a social network. The campaigns seek donations collected in the form of VAs issued by the social network. In particular, the influencer instructs his audience on how to purchase it, explains the benefits in terms of confidentiality, and points out reliable payment providers with deficient due diligence processes. The 'virtual currency' collected is then converted into VAs and disbursed to a virtual address belonging to the influencer. Every month, the influencer creates new crypto addresses to collect funds (nearly fifty in the space of a year and a half), to make the process as opaque as possible. The funds (equivalent to tens of thousands of euros) are stored for around a year before being transferred to individuals active in jihadist circles.

The first part of the investigation consisted of identifying the influencer's collection strategy, based on extensive open-source research (OSINT), in particular on encrypted messaging applications and on platforms selling telephone numbers and pseudonyms associated with this messaging application.

The second part of the investigation then focused on identifying the influencer's crypto addresses:

- Identification of addresses clusterised via blockchain analysis tools, belonging to the influencer and having similar characteristics (connection-log revealing a common geographical location of owners of the crypto addresses concerned).
- As many addresses were self-hosted, there was few possibilities for the FIU to obtain identification information, as it is the case with addresses hosted by a VASP.
- On the basis of the influencer's rare counterparts hosted by a VASP, the latter helped to identify the influencer through transmissions of unique transaction identifiers, and enabled deanonymization of counterparts.

Source: Tracfin, France

© FATF-OECD 2025

197. As these become more popular, accessible and profitable, terrorist organisations and individual terrorists have also adapted to exploit these features to raise funds and maintain profiles. Some jurisdictions report that terrorist organisations have benefited from fundraising campaigns launched with the use of trending social media features (i.e., filters and games) to generate money through TikTok's Effect Creator programme.

198. Some terrorist groups and individual terrorists designated under various national and/or supranational regimes have been reported to benefit from the above mentioned perks of paid premium accounts on platform X, formerly Twitter, both to get higher traction for posted videos promoting violence and propaganda, and to enable ads running in the replies to their posts, raising the possibility that they could get a cut of that ad revenue[166].

199. Research, in particular referring to big-brand advertisements appearing on posts by ISIL and EoRMT groups, indicates that terrorists may earn money through ad revenue under their popular videos or blogs[167]. Although several platforms have taken measures to ensure that monetisation function is disabled in case of violence or terrorism promoting content, gaps in controlling the functionality of this feature render it vulnerable to the risk of raising terrorist funding through social media videos, such as big-brand advertising and Super Chat payments.

5.2. Trade enabled fraud through social media

200. Social media platforms are increasingly integrating e-commerce functionalities, enabling direct transactions within the platform. This trend facilitates seamless shopping experiences, allowing users to purchase products without leaving the app. Features such as Instagram's Shopping Tags and Facebook's Marketplace exemplify this shift, empowering businesses, and creators to monetise their content directly. For instance, platforms like LinkedIn, Instagram, and Facebook allow companies to showcase their products and services. Platforms like Meesho and Shopsy enable small businesses to open digital stores and sell products directly through social networks.

201. Furthermore, and as recently noted by the FATF in its report on ML/TF in the art and antiquities market[168], the use of social media sites and messaging services in the trade of cultural objects has also developed rapidly over the last five years. Several jurisdictions as well as researchers have identified cultural objects, specifically antiquities, being sold through social media platforms by individuals who may have a connection with terrorists

[166] See, e.g., open-source reports by Tech Transparency Project—available at www.techtransparencyproject.org/articles (February 2024) and www.techtransparencyproject.org/articles (October 2023).

[167] RUSI, Global Research Network on Terrorism and Technology: Paper No. 10 Social Media and Terrorist Financing: What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better? (2019), Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks (2022) (see also, Alexi Mostrous, 'Big Brands Fund Terror Through Online Adverts', The Times, 9 February 2017; US House of Representatives Committee on Financial Services, 'Memorandum: February 25, 2021, NSIDMP Hearing Entitled, "Dollars Against Democracy: Domestic Terrorist Financing in the Aftermath of the Insurrection"', 22 February 2021, Megan Squire, 'Monetizing Propaganda: How Far-Right Extremists Earn Money by Video Streaming', conference paper, WebSci '21: 13th International ACM Conference on Web Science in 2021.

[168] FATF Money Laundering Terrorist Financing Art Antiquities Market (2023)

© FATF-OECD 2025

or terrorist organisations, or their facilitators[169]. The use of online facilitators to purchase or sell cultural objects also makes it easier for buyers and sellers to conduct cross-border transactions, and for marketplaces to circumvent the regulatory frameworks that have been put in place in some jurisdictions[170].

5.3. Formal and informal crowdfunding

202. Crowdfunding platforms enable fundraising project promoters to reach potential donors quickly and at low cost. FATF research has shown that crowdfunding, while a legitimate activity, has been exploited by various terrorist groups to raise money for TF purposes. Globally, the abuse of donation-based digital crowdfunding is most frequently observed in suspected TF cases.

203. The FATF identified donation-based crowdfunding as most likely to be exploited for TF purposes of all different forms of crowdfunding[171]. The four main typologies of crowdfunding abuse for TF purposes identified in the report are: abuse of humanitarian, charitable or non-profit causes; use of dedicated crowdfunding platforms or websites; use of social media platforms and messaging apps for purposes of crowdfunding; and the interaction of crowdfunding with VAs.

204. The report specifically notes that in the context of crowdfunding, terrorists rely on multiple methods to raise funds and may combine various techniques. For example, a fundraising campaign may be established on a dedicated crowdfunding platform, shared through social media, and collect payments in VAs. Following a crowdfunding campaign, terrorist entities and facilitators use various offline and online means to manage and move funds. In some cases, HOSSPs are used to disperse funds.

205. The common challenges echoed by national authorities include obtaining information to form or support TF suspicions given the fragmentary nature of data available to crowdfunding platforms and payment service providers used for transfer or withdrawal of funds; tracking the flow of money in foreign jurisdictions; identifying money receivers; and proving a terrorism link—especially in cases that do not directly involve designated terrorist organisations.

206. Humanitarian, charitable, and non-profit causes can serve as effective covers for financial solicitation and are, in some cases, exploited for TF purposes. The FATF report[172] identified three ways in which such abuse can occur: First, individuals unaffiliated with a registered charity or NPO may launch financial appeals under the guise of humanitarian or social causes, while the funds raised ultimately support terrorism-related activities or actors. Second, a registered charity may issue an appeal but fail to carry out the stated humanitarian activities, diverting all or part of the funds to TF. Third, there is a risk that NPOs crowdfunding for legitimate purposes may fall victim to extortion or skimming, particularly when operating in high-risk environments under the influence or control of terrorist groups.

207. A particular trend has emerged of funds being raised to sustain in or smuggle ISIL associated FTFs, and/or their family members, including children, from camps and prisons

[169] E.g., 2019 Report of the Antiquities Trafficking and Heritage Anthropology Research (ATHAR) Project—available at https://atharproject.org/report2019/

[170] For more details, please see section 7.g.

[171] FATF, Crowdfunding for Terrorism Financing (2023), page 38

[172] Op. Cit.

© FATF-OECD 2025

soon after the defeat of ISIL in the north-east of the Syrian Arab Republic in March 2019[173]. Some fundraising networks generated funds which were then transferred via hawala networks to the Hawl camp[174]. Fundraising campaign operators responsible for the campaigns display varying levels of sophistication, accepting a wide range of VAs. Fundraisers state on their online channels, groups, and accounts that the funds are sent to the camps to improve the detainees' conditions or to secure their release. The campaigns raise anywhere from twenty to tens of thousands of dollars, with individual donations ranging from tens to hundreds of dollars[175].

208. While these campaigns typically avoid displaying open support for ISIL to avoid detection and suspension by social media platforms and messaging apps, a closer look at their online content confirms their ideology and reveals the identifiers such as the use of specific religious terminology and images exclusively used by ISIL, or references glorifying their attacks[176]. The campaigns are often promoted by ISIL supporters online and are primarily in Arabic and English. Some campaigns are in other languages, including Russian, French, and German, indicating that they are focused on foreign women who had moved to ISIL territory before its collapse. Also, of these campaigns operate on multiple blockchains and employ a wide range of techniques for moving funds. These include the use of shared addresses (hosted and un-hosted), preferred wallet providers, temporary addresses, privacy coins, and cashout mechanisms.

209. The FATF report[177] also highlighted a recent investigation by the French financial intelligence which identified a typology whereby offline and online crowdfunding mechanisms were used to collect funds to finance the escape of female members of ISIL detained in camps in North-East Syria[178]. These calls for donations were complemented using digital tools, including promotion through social networks and encrypted messaging applications, and with the use of prepaid vouchers convertible into VAs and subsequently cashed.

210. With respect to EoRMT individuals and groups, FATF noted that they have been found to use dedicated crowdfunding platforms or websites to raise money for various activities, some of which may be protected by law (e.g., fundraising for legal fees, to support political campaigns, pay membership fees and fund protests). These actors may take advantage of crowdfunding for activities that promote hate or violence, but do not necessarily meet the threshold of terrorism.

---

[173] UN CTED Trends Tracker Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014-2024 (2024).

[174] Katherine Bauer and Matthew Levitt, "Funding in place: local financing trends behind today's global terrorist threat", 25 November 2020, page 59; Richard Hall, "ISIL suspects in Syrian camp raise thousands through online crowdfunding campaign (2019)—available member also United States, Department of Treasury, Office of Foreign Assets Control, "Treasury designates facilitation network supporting ISIL members in Syria", press release, 9 May 2022—available at https://home.treasury.gov, reiterated in ibid., Department of the Treasury, "2024 national terrorist financing risk assessment", February 2024—available at https://home.treasury.gov

[175] UN CTED 2024 Trends Tracker citing to TRM, "Fundraising campaigns for ISIL families: analysing the use of cryptocurrency", 12 April 2022—available at https://www.trmlabs.com/post/fundraising-campaigns-for-isis-families-analyzing-the-use-of-cryptocurrency

[176] Ibid.

[177] FATF Crowdfunding for Terrorism Financing (2023)

[178] FATF Crowdfunding for Terrorism Financing (2023), box 5.9.

© FATF-OECD 2025

Case study: Abusing social media fundraising instruments for TF purposes

In a recent investigation, FIU Thailand uncovered that a social media profile had launched fundraising campaigns to gather financial support for the families of deceased members of a Thailand insurgence group many of whom were designated under Thailand's Counter-Terrorist Financing law as individuals involved in acts of terrorism.

Beginning in 2021, the profile disseminated content that misrepresented religious principles to promote the insurgent cause and posted bank account numbers explicitly soliciting donations under the guise of humanitarian aid. Donors transferred funds via wire transfers and online banking platforms. The account holder later withdrew the funds and publicly shared images of the cash being handed over to the families, in an effort to reassure donors that the money was being used as claimed.

Between 2021 and 2023, the campaign raised over USD 300,000.

Source: Anti-Money Laundering Office, Thailand
Note: The case references to domestic designated individuals under Thailand legislation.

6. Virtual assets and virtual asset service providers

211. VAs have many potential benefits and dangers. Provided they are properly regulated, they have the scope to make payments easier, faster and cheaper, an provide alternative methods for those without access to traditional financial products. They are also vulnerable to abuse by terrorist financiers, to raise and move funds. Illicit actors, including terrorists, may favour using VA because of enhanced anonymity, opportunities to diversify funding sources or methods to move funds, greater speed of fund movements, the global reach of this technology, and the potential to send VAs in P2P transfers without the use or involvement of a VASP or other obliged entity[179]. As VAs have become more widely used in the licit economy and liquidity in VA markets has increased, terrorists have also improved their understanding of how to use VAs. Furthermore, basic use of VAs, such as low-level trading, are widely available via VASPs and can often be utilised with minimal technical knowledge or experience.

212. The exact scale of the misuse of VAs for TF purposes is still difficult to measure. As explained above, the use of VAs by terrorist groups and individual terrorists is overall on the increase, including in combination with other methods, and this is consistent with the overall increase in the use and popularity of VAs by the public. While several delegations consider the misuse of VA for TF is overall likely to remain lower compared to the use of other funding channels, such as cash and HOSSPs, some groups are already demonstrating a systemic use of VAs for their financing schemes, as it is the case with ISIL-K.

213. According to recent research, VAs have become a more important element of ISIL overall financial tradecraft. Blockchain analytics firms have reported donations being

[179] See also, UNSC Counter-Terrorism Committee, Non-binding guiding principles for Member States on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes, S/2025/22, January 2025, paragraph 11.

© FATF-OECD 2025

made to ISIL-K's media unit in Bitcoin, Ethereum and TRX (Tron), very likely in response to propaganda and recruitment efforts, and to an ISIL-K recruitment campaign in Tajikistan to the tune of approximately USD 2 million in USDT (Tron)[180]. Once in cash, ISIL-K can utilise couriers to run the money wherever it needs to go, to pay for goods or services rendered or to cover other costs such as salaries. Otherwise, hawaladars can hold funds in VAs in-trust for an intended beneficiary or transfer to someone else[181]. The UN 1267 Monitoring Team reports that some listed terrorist groups are promoting mandatory preliminary sharia assessments to establish permissible use of a specific VAs. Specialised channels, such as Crypto Halal and Umma Crypto, have been established on the Telegram application to enable channel moderators to control supporters' acquisition of specific liquid currencies and receive information on funds in their possession[182].

214. Much of the TF activity linked to VAs involves solicitation of funds and donations by individuals. As described in the previous two subsections, this may take the form of a crowdfunding campaign in which social media, encrypted mobile applications, or use of other internet-based crowdfunding features to disseminate a fundraising call requesting VA donations. In some cases, terrorist groups appeal overtly and directly to supporters and use propaganda outlets to circulate VA wallet addresses. In other cases, they may try to disguise the true purpose of the funds and utilise fraudulent charitable appeals or other pretences to avoid being detected or suspended by the platform. In such cases, instructions on how to make donations are communicated through private chats or other obfuscated methods. Indeed, detailed instructions to make payments through registering and replenishing digital wallets are routinely provided to transfer money through VAs.

215. Bitcoin remains the primary VAs used in TF-related fundraising campaigns. However, in recent years, as blockchains analytics and other investigative techniques have evolved to trace some VAs transactions, terrorists have increasingly diversified their VAs-based financing schemes (e.g., soliciting stablecoins[183] such as Tether's USDT[184] or Ethereum ETH). Information collected from private sector blockchain analytics companies through TPC also indicates an apparent shift from use of Bitcoin to the use of USDT. This shift, also signalled by some jurisdictions in relation to specific terrorist groups, is likely driven by the price fluctuations associated with Bitcoin, the lower fees associated with using USDT, and the outdated perception that it is harder to trace. Terrorist organisations and individuals are also known to have used anonymity-enhancing tools, including cryptographic technologies designed to obfuscate transaction details to raise and move funds. Such methods, like the use of mixers or anonymity-enhancing VAs, particularly Monero, can complicate investigators' ability to trace illicit funds. Increased use of single-use addresses, experimentation with decentralised exchanges and growing use of unhosted wallets have also been signalled.

216. Terrorists may use VAs for a range of purposes, including to move funds internationally (through VASP or P2P transfers), whether it was acquired through

[180] TRM Labs, 'New Evidence Confirms ISIS Affiliate in Afghanistan Accepting Cryptocurrency Donations', 21 December 2022, accessed 3 August 2023; TRM Labs, 'TRM Finds Mounting Evidence of Crypto Use by ISIS and its Supporters in Asia', 21 July 2023, accessed 3 August 2023.

[181] Project CRAAFT, The Islamic State in Afghanistan: A Golden Opportunity for a 'Golden Child' Stephen Reimer, Research Briefing No. 13, (2023), Jessica Davis, 'Cryptocurrency Meets Hawala', Insight Intelligence, 10 February 2022.

[182] S/2024/556, paragraph 94—available at: www.un.org.

[183] Stablecoins purport to maintain a stable value relative to some reference asset or assets.

[184] FATF Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Providers (2024)

© FATF-OECD 2025

donation campaigns or other means. VAs can also be used for the procurement of weapons, propaganda creation or dissemination, to finance the preparation and execution of terrorist attacks, or in some cases, to secure the release of detainees. Using VAs for goods or services likely will require converting it into fiat currency

217. Whether it is to conduct conversion operations, to transfer VAs or to address other needs, terrorists using VA often require the involvement of VASPs, such as VA exchanges or VA ATMs, or financial institutions. In some instances, terrorist used unregistered or unlicensed VASPs, such as local business offering informal conversion services in addition to hawala services. Identifying such unregistered or unlicensed VASP (including individual exchangers) can be helpful to understanding regional networks, including insights where terrorist actors are exchanging VAs for fiat currency. Importantly, some jurisdictions note that certain VASPs have deficiencies in implementing preventive measures. Furthermore, there are still a larger number of VASPs that are not subject to regulation as they are located in jurisdictions that have not implemented the FATF requirements for VA/VASP. As such, the uneven, and in many cases, inadequate, regulatory, and supervisory environment for VASPs in many jurisdictions has created opportunities for terrorists exploit the lack of a level playing field. Terrorist groups may seek out VASPs in jurisdictions with weak or non-existent AML/CFT controls to conduct their activities.

218. The fifth update on the implementation of the FATF Standards on VA/VASP[185] and VASPs, published in June 2024, highlights the fact that several governments have yet to take significant steps to regulate the sector and that there is a long way to achieve a global coverage of AML/CFT regulation in this sector.

Case studies: Abuse of VA/VASPs for TF purposes

1) International TF network using exclusively VAs:

In 2023, 'Operation Grafos' targeted an individual in Spain identified as a key actor within a transnational TF network linked to ISIL and AQ. The investigation revealed the network's exclusive use of VAs to raise, layer, and transfer funds across multiple jurisdictions, employing sophisticated methods of financial obfuscation.

The network sourced VAs through various means, including VA coupons purchased in tobacco shops in France and online donation campaigns denominated in cryptocurrency. These assets were transferred across numerous e-wallet addresses to evade detection. The funds typically originated as Bitcoin, were subsequently converted into stablecoins (e.g., USDT), and ultimately exchanged into fiat currency, predominantly Turkish lira.

Investigators observed high volumes of transactions lacking clear commercial or economic justification, alongside rapid and circular movement patterns designed to obscure the origin and destination of funds. Frequent conversions between cryptocurrencies further complicated tracing efforts. The complex, cross-border

[185] FATF report on Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Assets Service Providers, (2024)

© FATF-OECD 2025

structuring of VA transactions presented a high degree of anonymity, requiring advanced blockchain analytics and tracing techniques.

The case was identified through coordinated efforts involving Europol, Spain, France, Sweden, and US authorities. Digital surveillance and enhanced VA-tracing tools uncovered layered transaction flows across three blockchain networks. Europol's Terrorist Finance Tracking Program (TFTP) enabled secure, cross-border intelligence sharing, helping to map the financial network. Spain's Guardia Civil led the investigation under judicial oversight and, with Europol's support, arrested the suspect, who was subsequently placed in pretrial detention on TF-related charges.

Source: Guardia Civil, Spain, and Terrorist Finance Tracking Program (AP TFTP), Europol. See: www.interior.gob.es

2) Abuse of VASP to transfer VAs to high-risk jurisdictions:

In 2019 and 2022, FIU Belgium referred two separate cases to the Federal Prosecutor's Office involving Belgian nationals who transferred VAs from Europe-based VASPs to Middle East-based VASPs.

The first case involved two French nationals whose Keplerk accounts were funded via prepaid Bitcoin vouchers. These vouchers were purchased with cash by unidentified individuals at a tobacco or night shop in Belgium. The credited amounts were subsequently transferred to Turkish-based VASPs—Paribu and BTC Türk. These platforms generated encrypted messages, which were relayed by intermediaries to recipients in conflict zones. Upon confirmation, the vouchers' value was disbursed in fiat currency. The network's structure indicated reliance on intermediaries and exchange offices in Syria, particularly in Idlib and the al-Roj camp. Communication and coordination were conducted via instant messaging platforms such as Telegram and WhatsApp, which were also used to share testimonials, operational instructions, and contact details.

The second case concerned a Belgian national who transferred VAs through BitPanda GmbH, a licensed Austrian VASP, to a Middle East-based VASP—Bitcoin Transfer, reportedly operating in Idlib—and to an NPO suspected of links to Hayat Tahrir al-Sham (HTS) and Al-Qaida. The transactions suggested potential support for ISIL-affiliated networks.

Source: FIU Belgium

3) Cross-border VAs transfers linked to TF

A VAs exchange reported suspicious transactions involving two individuals, one citizen of Tajikistan, the other from a jurisdiction in Africa. It was identified that one of the individuals regularly transferred significant sums in VAs to accounts associated with the other. The ensuing investigation revealed large-scale activity involving VAs, including cross-border transfers to high-risk jurisdictions and transactions on a cryptocurrency exchange. Further analysis uncovered that one of the cryptocurrency wallets had been featured on a Telegram channel known for disseminating radical content, including videos of ISIL militants pledging allegiance and appeals for financial contributions to support terrorist activities. In addition to the VA transfers, the suspects were also linked through transactions conducted via bank cards and money transfers executed without the opening of

© FATF-OECD 2025

formal accounts. As a result of the investigation, the FIU Tajikistan referred the case to LEAs, leading to the initiation of criminal proceedings under terrorism-related legislation. The assets of one suspect were frozen, and their cryptocurrency holdings were confiscated through coordinated efforts between the private sector and LEAs. Procedures for the recovery of these assets are currently being finalised as of 2025.

Source: Tajikistan

219. While many terrorist organisations have experimented to some degree using VAs, others have demonstrated more technical capability and further embedded them with their financial structures. In 2024, ISIL-K has increasingly used VAs for organisational transfers and to collect donations from international supporters often claiming support for ISIS-associated families in detention camps, which were later used to operate, recruit or finance attacks. For example, at least part of ISIL's March 2024 Moscow Crocus Hall attack was funded through VAs collected and transferred through various ISIL entities. Much of ISIL-K's international donations are received in VAs, and they use their official media outlet, Voice of the Khorasan, to solicit these donations. Additionally, ISIL has expanded its use of VAs in Asia and Africa. Several cases where ISIL affiliates used donation campaigns linked to Monero wallets and provided instructions on how to use them were also reported in 2023[186].

220. Some EoRMT groups have also sought to solicit or transfer funds in VAs pseudonymously. As EoRMT groups have increasingly been banned from various fiat payment platforms for violating terms of service, some have turned towards using VAs. However, as many EoRMT groups obscure their identities and objectives by using legal entities and , their activity involving either VAs or other payment mechanisms may be fully licit depending on what the funds are being used for.

221. Related to the analysis above on the use of social media and messaging services, the introduction by some communication apps of features allowing users to send, receive and exchange VAs, as well as to trade VAs for fiat, has facilitated the transfers to TF campaigns. In-app wallets mostly lack CDD and could therefore become a concerning trend.

222. Despite heightened public attention to these new technologies, there remain limitations with the use of VAs for TF, and local factors will play a role in determining whether using VAs makes sense to transfer or raise funds. For example, converting VAs to fiat currency is not always convenient, and this remains an impediment to more widescale adoption as it may be a necessary step depending on the desired use of the funds. Arguably, the volatility of the value of VAs can introduce additional risks for terrorist groups or violent extremists, who may prefer to rely on more stable and traditional forms of value such as cash.

223. Certain elements of VAs may support tracing funds associated with TF. When VA transactions occur on public blockchains, anyone with internet access can view the

[186] United Nations, thirty-fourth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning Islamic State in Iraq and the Levant (ISIL), Al-Qaida and associated individuals, groups, undertakings and entities (S/2024/556), paragraphs 96-97. Submissions received during targeted public consultation also indicate use of Monero by several ISIL-affiliated groups in Afghanistan, India, Pakistan, and the Philippines.

© FATF-OECD 2025

pseudonymous transaction data in a public ledger for the blockchain. Public ledgers can support investigations in tracing the movement of illicit funds. However, there are some limitations due to the pseudonymous nature of the data, challenges associated with the use anonymity-enhancing techniques, and activity occurring of-chain. Also, law enforcement relies heavily on the limited number of providers offering blockchain analytics tools. Still, public blockchain data can support investigations of TF in VAs and emphasizes the urgent need to ensure the FATF Standards for VAs/VASP are implemented without delay and the critical role that VASPs may play in acting on law enforcement information to disrupt TF.

Case study: Creation of VAs by a domestically designated EoRMT group

An EoRMT group in South Africa created their own stable coin pegged at a 1:1 ratio with the local currency (South African Rand/ZAR). The stable coin was managed through an online application and enabled the group to use the digital asset as they would cash. The application reportedly deleted transaction data after a short period and provided anonymity to group members and their supporters. Investigations in South Africa identified that the group raised funds of ZAR 268,000 (approximately USD 13,636) using this methodology. Although relatively low in value, the use of stable coins demonstrates that groups are evolving their methods to raise funds, and this case also showed the ability to connect with supporters outside South Africa with financial support reportedly provided by individuals in the United States, United Arab Emirates, Australia, and Switzerland.

Source: South Africa

6.1. E-commerce platforms and online marketplaces (EPOMs)

224. Terrorists have been reported to abuse EPOMs, which are occupying an ever-growing position in worldwide economic landscapes, for various purposes.

225. The RTMG recently discussed how EPOMs also play an enabling role for terrorist and TF purposes[187], noting in particular that EPOMs can impact the ML/TF landscape due to their transnational access and reach, which is enabled and made complex through their de-centralised and international operations. Criminals and terrorists can pose as multiple buyers and sellers (e.g., fraudulent/complicit online shop fronts) on the EPOMs, and use trade-based ML/TF techniques, such as over/under invoicing, to transfer value (goods and funds) between each other.

226. Terrorists have used EPOMs platform for their operational procurement (equipment, weapons, chemicals, 3D-printing material), including because of the discretion they can offer over purchasing such items in a physical shop. EPOMs can also be used by terrorists to sell items to finance their projects and operations, including lower value items that were previously not in demand[188]. EPOMs can be used to sell items obtained through wildlife exploitation or stolen cultural artefacts. In cases of small cells

[187] FATF/RTMG(2025)2 (non-public).
[188] Europol (2021), European Union Serious and Organised Crime Threat Assessment (SOCTA), www.europol.europa.eu

© FATF-OECD 2025

and lone actors relying on self-financing, EPOMs can be used to sell personal items. EoRMT groups have been observed using EPOMs to sell merchandise and propaganda items.

227. Finally, EPOMs can be used for fund-moving purpose inspired by trade-based money laundering schemes. Traded goods can indeed offer disguise to value being transferred from an accomplice to another member of the network. In such scheme, the first actor would purchase items, send them to his accomplice through an EPOM, for the latter to sell items in another jurisdiction and use profit to finance terrorism.

© FATF-OECD 2025

Case studies: Misuse of e-commerce platforms for TF purposes

Use of e-commerce platforms, social media, and VAs to finance and promote ISIL activities:

D.E. was arrested on August 2023 for involvement in terrorist activities and financing, particularly in support of ISIL and the dissemination of extremist propaganda via social media platforms such as Facebook and Telegram. D.E. operated multiple e-commerce accounts under various aliases and maintained several bank accounts. He received funds through platforms known to facilitate the sale of weapons, as well as from individuals linked to ISIL networks in Syria. Through his social media presence, D.E. actively promoted jihadist propaganda by sharing ISIL-related content and updates. His accounts were also associated with the sale and purchase of weapons and ammunition. Additionally, D.E. provided financial support to ISIL supporters in the al-Hol and al-Roj camps in Syria by channeling funds through APM, a fundraising organisation established by ISIL sympathizers in Indonesia. The funds were exclusively directed to ISIL affiliates.

After the arrest of D.E., the TF investigation against the APM network was expanded and led to the arrest of N.K. (a pro-ISIL terrorist financier) in December 2023. Previously in mid-2020 N.K., together with his wife pledged allegiance to ISIL through a social media post and declared their supports to ISIL ideology and operations. The subject managed to create and to lead three pro-ISIL local cells in different regions of Indonesia. He was able to utilize social media platforms and messaging applications to spread the radical ideology and propaganda, to recruit ISIL sympathizers, and to raise funds in Indonesia. In particular, N.K. and his wife also organised funds raising activities dedicated to channel funds to terrorists in Syria through the APM network, by administrating a Telegram channel. N.K. was in contact with an Indonesian terrorist located at the al-Hol Camp in Syria to arrange the funds transfers. Within the period of November 2021 until December 2023, N.K. was able to transfers funds in total of IDR 85,216,310 (approximately USD 5,192). Besides using banking system and money remittance services, N.K. also instructed his daughter to transfer funds in the form of VAs (22,114,039 BIDR converted to 1,412.30 USDT) to two pro-ISIL wallet addresses held in Syria.

Source: National Counter-Terrorism Agency of the Republic of Indonesia (BNPT) and FIU Indonesia (PPATK)

Use of e-commerce platform in the procurement of materials for a terrorist attack in India:

In February 2019, a suicide bombing targeted a convoy of Indian Security forces, resulting in the deaths of forty soldiers. India's authorities concluded that the attack was orchestrated by Jaish-I-Mohammed (JiM). Investigations revealed the cross-border movement of a large quantity of explosives into India. Notably, a key component of the improvised explosive device used in the attack— aluminum powder—was procured through the EPOM Amazon. This material was used to enhance the impact of the blast. As a result of the investigation, 19 individuals were charged under relevant provisions of the Unlawful Activities (Prevention) Act, including sections related to TF. Among those charged were seven foreign nationals, including the suicide bomber. LEAs also recovered moveable and immovable assets connected to the attack, such as vehicles and terrorist hideouts.

Source: India

6.2. *Online video games and gaming platforms*

228. Gaming platforms are increasingly becoming spaces terrorist and extremist actors use to exploit to disseminate propaganda, recruit members, incite and engage in radicalisation activities, communicate and sometimes fundraise[189]. This underscores the need to better understand the challenges and opportunities for safeguarding these digital environments.

229. Research into the financial crime risks of in-game purchases has revealed significant ML concerns[190]. This highlights the potential nexus between TF and ML techniques used to either move or layer funds using gaming platforms.

230. There is some degree of scepticism on the scalability of video games for TF, as these platforms may not yet offer transactions of sufficiently value to serve as a primary tool for such activities. Also, fees can be quite high to conduct transactions on gaming platforms, reducing this attractiveness of the channel for TF. However, data collected on microtransactions and the sale of digital video game items from the past several years indicates that virtual transactions can be lucrative[191]. Due to the lack of sufficient oversight and relative ease of exploitation of these systems, criminals can quickly launder large amounts of money through thousands of small transactions—a method some terrorist groups are known to use[192]. Furthermore, in-game voice and text chats that are known to have been used to recruit and incite lone-actor attacks can also provide terrorists with relatively secure platforms to solicit donations and provide guidance on how to conduct financial transactions securely to avoid detection[193].

231. Some occurrences of terrorist groups, including EoRMT organisations as well as Hezbollah[194], creating and selling their own video games, for both propaganda and financing purpose, can be found in open—source research materials[195]. Transactions can also take place through in-game items, as it has been observed by some EoRMT groups. Game elements can indeed be purchased and donated to other player, without much traceability of transactions.

232. In another trend, some games offer options of reenacting a specific attack or allowing user to play from the perspective of terrorists. While such options can often be downloaded for free, the sales of the games themselves do generate revenue for their developers[196]. The revenue can also come from donations during the gameplay.

---

[189] King's College London, Global Network on Extremism & Technology (GNET), "30 Years of Trends in Terrorist and Extremist Games", Emily Thompson and Galen Lamphere-Englun, November 2024.

[190] Video Games Might Matter for Terrorist Financing | Lawfare ; Project CRAAFT, "Virtual Threats: Terrorist Financing via Online Gaming", Gonzalo Saiz, 2025 available at https://static1.squarespace.com

[191] See also, Project CRAAFT, "Virtual Threats: Terrorist Financing via Online Gaming", Gonzalo Saiz, 2025—available at https://static1.squarespace.com

[192] Ibid.

[193] Project CRAAFT, "Virtual Threats: Terrorist Financing via Online Gaming", Gonzalo Saiz, 2025—available at https://static1.squarespace.com

[194] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[195] GNET-37-Extremism-and-Gaming_web.pdf; 30 Years of Trends in Terrorist and Extremist Games – GNET

[196] Project CRAAFT, "Virtual Threats: Terrorist Financing via Online Gaming", Gonzalo Saiz, 2025—available at https://static1.squarespace.com

© FATF-OECD 2025

233. ISIL has been reported to have used the exchange of video gaming points to fiat currency, demonstrating the potential for abuse within these digital environments[197]. Similarly, Al-Shabaab[198] is reported to have abused an online gambling platform registered in the Caribbean for TF, underscoring the risk that arises across distant jurisdictions and the resulting challenges for detection and enforcement. There have also been reports of minors being involved in in-game transactions ultimately benefiting terrorists.

Case study: Exploitation of gaming platforms for TF purposes

In 2018, the South African Financial Intelligence Centre (FIC) identified a bank account used to make extensive payments to the PlayStation Network Online Platform. Such platforms, often operating outside the oversight applied to mainstream social media, can serve as enablers for terrorist activities and TF by providing unmonitored communication channels.

FIC's analysis of the account, linked to a suspected individual, revealed multiple red flag indicators suggesting potential involvement in extremist activities. These included irregular transactions labelled as "salary", the purchase of an iPhone, a significant payment for an identification document, and consistent online activity on the PlayStation Network. The individual was also flagged by the FBI for alleged terrorist activity in Somalia and suspected ties to ISIL.

Further investigation showed that the suspect used a licensed local money remitter to send 57 low-value transactions to recipients in Somalia and Kenya. These transactions originated primarily from the Fordsburg and Mayfair areas of Johannesburg, known hubs of remittance activity.

Source: South Africa.

7. Methods based on the exploitation, trade and trafficking of natural resources

234. In countries where the government lacks effective control of territory and its resources, the natural resources sector may be vulnerable to exploitation for TF[199]. Terrorist organisations may use these resources to raise funds by controlling or exploiting a wide range of vulnerable resources, including gas, oil, timber, precious metals and stones, wildlife, fishing and agricultural goods, and charcoal.

235. Terrorist engagement in legitimate economies related to natural resources is strategically important for these groups, both to generate regular income and to further

[197] UN 1267 Monitoring Team

[198] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[199] FATF Emerging Terrorist Financing Risks (2015)

© FATF-OECD 2025

diversify the sources of funding[200]. These sectors represent a profitable source of revenue and may also be appealing because of weak regulation in the sector. There is also a higher TF risk in regions with a history of weak institutions, political instability, conflict areas and those regions rich in untapped natural resources. Some of the examples below entail taking control of parts of the local economies upon which communities subsist.

236. The UNSC has continuously expressed concern at the use of the proceeds from the illegal exploitation and trafficking of natural resources by armed groups, terrorist groups and criminal networks supporting them[201]. In July 2021, FATF noted that "there is evidence that armed groups and terrorist organisations do, to varying extents, rely on certain environmental crimes to support and finance their operations"[202]. In July 2022, UN CTED issued a Trends Alert highlighting how terrorist groups can strategically diversify their funding streams into a variety of both illicit and licit activities relating to various types of natural resources[203].

237. While the exploitation, trade, and trafficking of natural resources by terrorist groups primarily concern jurisdictions where such resources are sourced, these TF schemes should also be of concern to third jurisdictions—including international and regional financial centres—where substantial proceeds may be transferred or processed. This exploitation is likely to involve international private actors, such as FIs operating in the commodity sector, insurance companies engaged in transportation, companies consuming commodities, supply chain infrastructure providers, as well as legal professionals and accountants providing services to these entities.

7.1. Oil and gas exploitation, trade, and trafficking

238. In the Syrian Arab Republic and Iraq, ISIL was able to generate considerable income from the production of, and trade in oil and natural gas in areas that it controlled predominantly in 2014 and 2015[204]. Despite ISIL's loss of control over territories in this region and the consequent drastic reduction in its access to oil and natural gas fields, FATF has noted funds being generated through extortion of oil networks in eastern Syrian Arab Republic as late as 2021[205]. Cash reserves accumulated through the earlier exploitation and trade may still be available to the terrorist group[206]. In the east of the Syrian Arab Republic, ISIL operations against SDF continued, many targeting fuel trucks in Dayr al-Zawr Governorate to raise money by extorting oil traders[207].

---

200 UN CTED 2022 Trends Alert Concerns over the use of proceeds from the exploitation, trade, and trafficking of natural resources for the purpose of terrorism financing (2022)

201 For example, see resolutions 2195 (2014), 2462 (2019), and 2482 (2019).

202 FATF Money Laundering from Environmental Crime (2021), page 8 "environmental crime, particularly mining, is a profitable tool for insurgent groups in conflict with the central government authority and for terrorist organisations operating in resource-rich jurisdictions where there is instability. Public reporting by Governments and NGOs has noted that these groups will engage in environmental crime as a means of raising revenue or as a direct means of value transfer/payment for goods (e.g., guns and drugs)".

203 CTED 2022 Concerns over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources for the Purposes of Terrorism Financing (2022).

204 Ibid.

205 FATF, "FATF Public Statement on the Financing of ISIL, Al Qaeda and Affiliates" (2021).

206 E.g. in April 2021, a sum equivalent to USD 1.7 million in buried USD and Iraqi dinar bank notes, as well as gold and silver, were seized in Mosul (S/2021/655, paragraph 65).

207 UN 1267 Monitoring Team S/2025/71/Rev.1, paragraph 60

© FATF-OECD 2025

239. Because of the skills and resources required to exploit oil and gas, it is difficult for terrorist groups to produce and refine oil unless a considerable amount of territory is controlled. However, AQAP continues to attempt to establish control over ports along the Gulf of Aden, and oil and gas infrastructure facilities[208]. In their 2021 report to the President of the UNSC, the members of the Panel of Experts on Yemen noted that the Houthis[209] were closer to taking control over important oil and gas wells[210]. Their networks also rely on various shipping companies, vessels, and facilitators to sell and ship commodities, including oil and petroleum products, generating revenue. Their control over port infrastructures in Yemen is also a source of revenue, including revenue derived from petroleum activities.

7.2. Agriculture, livestock and fishing exploitation, trade and trafficking

240. Natural resources used for agriculture and fishing (e.g., livestock, red pepper, cocoa, coffee) have been exploited by terrorists for the purposes of generating income[211].

241. In the Lake Chad Basin region, where the economy is largely based on agriculture and fishing, recurring cases of livestock theft and illegal trafficking of fish products by Boko Haram have been identified[212]. Terrorists operating in this area have also derived income from the trade in smoked fish and red pepper, as well as through the extortion of communities involved in farming and fishing activities[213]. ISWAP, in particular, has generated funds locally from farming activities such as growing red chillis for sale to countries neighbouring Lake Chad[214]. The group has also been reported to engage in trading in vegetable oil, relying on the local production of large quantity of groundnuts[215]. ISWAP also profits from renting fishing and passenger boats to the locals[216]. Notably, ISWAP is estimated to earn up to USD 116,000 daily from issuing fishing 'permits'[217].

208 Twenty-ninth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), (S/2022/83), paragraph 43

209 Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

210 Final report of the Panel of Experts on Yemen (S/2021/79), table 4.1. Council resolution 2624 (2022) subsequently called the Houthis a terrorist group and added the group as an entity to the Yemen sanctions list.

211 UN CTED Trends Alert: Concerns Over the Use of Proceeds from the Exploitation, Trade, and Trafficking of Natural Resources for the Purpose of Terrorism Financing, citing to Petrich, Katherine "Cows, Charcoal, and Cocaine: Al-Shabaab's Criminal Activities in the Horn of Africa", The Linkages between Organized Crime and Terrorism, Studies in Conflict & Terrorism (2022)

212 FATF, GIABA and GABAC joint report on Terrorist Financing in West and Central Africa (2016)

213 Samuel, Malik "Economics of terrorism in Lake Chad Basin" (2019), Institute for Security Studies.

214 UN 1267 Monitoring Team

215 Institute for Security Studies (ISS), Boko Haram's deadly business: an economy of violence in the Lake Chad Basin by Malik Samuel (2022)

216 UN CTED 2022 Trends Alert, Op. cit.

217 Ibid.

© FATF-OECD 2025

242. In 2021, the UN Panel of Experts on Somalia assessed that Al-Shabaab[218] generated funds through, inter alia, a range of illicit taxation on agriculture (farms and farming produce) and livestock (primarily cattle, camels, and goats)[219].

243. There is also an emerging nexus between highway banditry, cattle rustling and TF. For example, in the Lake Chad basin cattle rustling remained a prevalent method of generating revenue, with some of the stolen livestock sold in local markets[220]. Various terrorist groups, including ISIL in Iraq, Boko Haram and Al-Shabaab[221], were reported to collect zakat taxes on herders[222]. Proceeds from cattle rustling are also often used to buy weapons for perpetrating extortion rackets as a source of revenue for the operations and other criminal activities they are engaged in. Conversely, stolen or raided weapons are used in conducting further criminal activities such as smuggling of timber, and trafficking to raise revenue. Revenues from cocoa and coffee have also been linked to TF[223]. Some cultivation, harvest, sale and smuggling of cocoa linked to ADF[224] were also reported in 2020[225].

244. Groups designated as terrorist organisations at the domestic level by the Palestinian Authority, have reportedly established private enterprises involving livestock farming and the development of large-scale agricultural projects, such as fruit, vegetable, and palm tree plantations as means of funding[226].

[218] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[219] 2021 United Nations Panel of Experts on Somalia report to the Chair of the Security Council (S/2021/849)

[220] S/2025/71/Rev.1, paragraph 105

[221] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[222] S/2025/71/Rev.1, paragraphs 105-106, 108

[223] UN CTED 2022 Trends Alert, Op. cit.

[224] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[225] Midterm report of the Group of Experts on DRC, (S/2020/1283), see Summary.

[226] These groups include Shuvi Eretz Outpost, Tirzah Valley Farm, Meitarim Outpost, Hilltop Youth, Price-Tag (TAG MEKHEIR). These organisations are designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

© FATF-OECD 2025

Case study: Dismantlement of a network providing funds, food, and logistics to terrorist operatives in Mozambique

In 2023, Mozambique authorities convicted several individuals for supporting ASWJ[227] by gathering intelligence on the village of Mocimba da Praia on behalf of the group's leadership. They were also accused of recruiting young people to join the group and providing supplies—such as food and operational goods—to ASWJ operatives in remote areas.

In March 2023, a joint operation by the Mozambique Defense and Security Forces led to the neutralisation of two individuals found in possession of a large quantity of food products in a village known for frequent terrorist activity. The defendants admitted that the supplies were intended for an ASWJ operative awaiting delivery at a pre-arranged location. One defendant revealed he was the nephew of an ASWJ leader and had been instructed to purchase a cell phone for encrypted communication via WhatsApp and Telegram and await further instructions on fund distribution.

In June 2023, the same leader instructed the defendant to receive MZN 885,500 (USD 13,862) from an intermediary and deliver it to a member of the group in the village. The defendant was arrested during the transaction. Investigations confirmed that the funds were intended for the purchase of a sailing vessel, a house, and the construction of a tent, with mobile communications revealing that proceeds from fishing activities were earmarked for the group's maintenance and operational costs.

The investigation revealed that funds were transferred between the group's leader and the defendants using both electronic money and physical cash transportation. The defendants were sentenced to 28 to 30 years in prison, and the seized funds were confiscated for the benefit of the Mozambique State.

Source: LEAs and Public Prosecutor´s Office, Mozambique.

7.3. Wildlife exploitation, trade, and trafficking

245. Wildlife trafficking (which is among the most lucrative criminal activities worldwide) has been previously reported as a source of funding for terrorist organisations

[227] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States. This applies for all references to ASWJ in the text box.

© FATF-OECD 2025

such as Boko Haram, Al-Shabaab[228], the Lord's Resistance Army[229], and others[230]. In 2017, GABAC raised concerns over the potential linkages between TF and environmental crime, including the sale and exchange of protected species such as elephant tusks[231]. ASWJ[232] has also been reported as implicated in smuggling hunting trophies. More recently, researchers and analysts appear to be taking a more cautious approach as to the scale of these linkages[233]. However, they seem to agree that, while this might not have been a primary source of financing for these groups, some instances have indeed occurred.

246. UN CTED has also noted some examples under investigation by national authorities, within the framework of recent country assessments, including poaching, smuggling of wild fauna and flora, and misappropriation of funds related to national parks[234]. Moreover, there appear to be more intricate linkages between wildlife crimes and other profitable criminal activities used by terrorists to generate profit. For example, INTERPOL suggests that illegal gold miners' settlements in forested areas, particularly in Central Africa, can foster the development of poaching of protected species, and other environmental crimes[235].

7.4. Precious metals and stones exploitation, trade, and trafficking

247. Delegations have reported the mining of gold and other precious metals as an increasingly important source of TF for terrorist groups, notably global affiliates of ISIL and AQ in Africa, and noted that rare earth metals were also being excavated to support regional terrorist groups[236]. Over the past decade, artisanal mining of gold, tin, and

[228] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[229] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[230] See e.g., the analysis of the United States Institute of Peace: Wildlife Poaching and Trafficking: Combating a Source of Terrorist Funding (2018), National Geographic, How Killing Elephants Finances Terror in Africa (2015). See also the record of the Hearing before the Subcommittee on Terrorism, Non-Proliferation and Trade of the Committee on Foreign Affairs of the US House of Representatives: Poaching and Terrorism: a National Security Challenge (22 April 2015).

[231] GABAC, "The financing of terrorism in Central Africa" (2017).

[232] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[233] See e.g., https://news.mongabay.com/2022/02/links-between-terrorism-and-the-ivory-trade-overblown-study-says/ (February 2022) and sources cited therein. The FATF report on Money-Laundering and the Illegal Wildlife Trade (June 2020) does not address the links between Illegal Wildlife Trade (IWT) and terrorism financing, stating that "current evidence suggests that this is not yet a widespread typology" (https://www.fatf-gafi.org/media/fatf/documents/Money-laundering-and-illegal-wildlife-trade.pdf).

[234] UN CTED 2022 Trends Alert.

[235] INTERPOL, "Analytical report: Illegal gold mining in Central Africa" (2021), page 34

[236] UN CTED 2022 Trends Alert; Twenty-ninth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning ISIL (ISIL), Al-Qaida and the Taliban and associated individuals and entities, February 2022 (S/2022/83).

© FATF-OECD 2025

tungsten has increasingly supported ADF[237] and the ISIL groups operating in Central Africa, with occurrences rated as common.

248. ISIL affiliates with an established presence in Africa have exploited the goldmining business not only by extorting gold miners working in unregistered mines, but also by engaging smugglers to move the gold from remote mining sites to trade points, and even using existing smuggling routes to sell gold at international trading hubs[238]. Illegal mining operations are profitable and attractive as gold is sold at a lower price than the legal gold market.

249. In Latin America, risk assessments of the gold sector have underlined its vulnerability to TF, particularly in Colombia and Peru[239]. A report by FATF and APG described a case study of a terrorist group in Colombia whose modus operandi consisted of taking control of territories where gold mines were located by extorting and coercing the owners to transfer the ownership titles of the land. Part of the gold produced illegally by the terrorist group was sold to legal businesses through cash transactions with a view to concealing its provenance. The profits were then used to buy equipment, munitions, medicines, and other supplies needed to continue with the group's terrorist activities[240]. Israel reports that Iranian Quds Force operatives acquire gold in Venezuela, smuggle it via airlines, and sell it in the Middle East, with profits transferred to Hezbollah[241] to finance its activities.

250. In Burkina Faso, Mali, and Niger, the gold rush is offering a new source of funding for terrorist groups, particularly in the Liptako-Gourma region, as the groups seek financing opportunities that are sustainable to finance their long-term activities, easily accessible, and available at the lowest risks of detection and disruption. The Islamic State in the Greater Sahara (ISGS) and JNIM are reportedly fighting in the Gourma sector of Mali, in part for control of gold extraction areas where the groups impose illegal taxation on small-scale gold miners for protection or to collect zakat. Affected regions include Kidal in the north of Mali (involving JNIM fraction groups such as Ansar Edine); Bongou and Soum in Burkina Faso (involving groups such as Ansar al Islam); and Kombongou in Niger (areas that have also suffered a number of terrorist attacks). The local communities are particularly vulnerable as they live in isolated areas with a limited law enforcement

[237] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[238] UN CTED 2022 Trends Alert citing to "Getting a grip /on Central Sahel's Gold Rush" (2019), International CrISIL Group.

[239] For Colombia, see of the International Monetary Fund (IMF) (2018) and Colombia's "Report on measures Peru conducted a "Sectorial Assessment of the ML/TF risks of the mining sector" (2017). See also discussions of the Joint special meeting of the Counter-Terrorism Committee, the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning ISIL (ISIL) Al-Qaida and associated individuals, groups, undertakings and entities; and the Security Council Committee established pursuant to resolution 1988 (2011) on "The nexus between international terrorism and organized crime" (26 April 2019).

[240] FATF and Asia/Pacific Group of Money Laundering (APG), Money laundering and terrorist financing risks and vulnerabilities associated with gold" (2015), case study 10, page 16.

[241] Organisation under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

© FATF-OECD 2025

presence. In DRC, ADF[242] has reportedly been involved in the illegal exploitation of gold mines near Bialose village.

251. Firearms operation (Operation KAFO II) coordinated jointly by INTERPOL and UNODC in late 2020 in the Sahel noted a terrorism-financing trend following the seizure of more than 40,000 sticks of dynamite and detonator cords, which were believed to be intended for illegal gold mining for armed terrorist groups in the Sahel[243].

252. In Mozambique, Cabo Delgado serves as one of the economic corridors for the region, bringing the growing risk that the presence of ISIL associates, notably the ISIL groups operating in Central Africa, have significant implications for illicit activities in the area, including the trade in gold and other precious metals or stones[244]. ASWJ[245] is also actively involved in illegal mining activities, with Mozambican forces recording instances of ASWJ members found in possession of metals and precious stones. Estimates suggest that ASWJ has generated approximately USD 30 million from ruby mining alone.

253. However, these trends vary by region and subregion. For example, whereas in West Africa the linkages between illegal gold mining through criminal networks and terrorist groups are growing clearer, these linkages are not as evident (although by no means absent) in Southern and Central Africa[246].

254. Besides generating profit from mining, terrorist organisations can also derive revenue from extorting miners and mining firms, as well as by taxing smugglers or transport companies. Suspicions were shared of ASWJ[247] encouraging local community members to obtain mining licences, in order to then derive profit to be made available to the terrorist organisation. As noted in the 2025 Global Terrorism Index[248], most of the time, terrorist groups in the Central Sahel don't directly extract, trade, or smuggle gold themselves. Instead, they control the areas where artisanal gold mining happens and collect taxes from miners.

---

[242] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[243] INTERPOL and UNODC "International operation disrupts supply of firearms to terrorists" (2020).

[244] UN CTED 2022 Trends Alert; International CrISIL Group "Stemming the insurrection in Mozambique's Cabo Delgado" (2021).

[245] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[246] UN CTED 2022 Trends Alert citing to Global Initiative Against Transnational Crime, "Insurgency, illicit markets and corruption: The Cabo Delgado conflict and its regional implications" (2022).

[247] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[248] Global Terrorism Index 2025 , page 52.

© FATF-OECD 2025

7.5. Timber and charcoal exploitation, trade and trafficking

255. Timber logging has also been reported as a funding source for JNIM. ADF[249] and the ISIL groups operating in Central Africa have been linked to illicit timber logging, particularly of rosewood, within territories under their control, with this activity occurring at a common level. Estimates suggest that ADF earns approximately USD 3 million annually from timber trafficking[250]. ASWJ[251] generates income through timber logging and participates in the illegal wood and charcoal trade, both rated as common occurrences.

256. Cases of production, taxation, and extortion of charcoal represent a further instance of the use of natural resources as revenue by terrorist organisations, including Al-Shabaab[252] in Somalia, where a profitable charcoal smuggling network brings in millions of dollars each year.[253] Other terrorist and armed groups in Africa (including in Central African Republic, DRC, Mali, and Sudan) have generated revenue from the illegal or unregulated charcoal trade[254].

[249] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[250] UN CTED 2022 Trends Alert; Daghar, Mohamed; Chelin Richard; Haji Mohamed, "Expansion of the Allied Democratic Forces should worry East Africa" (2022), Institute for Security Studies.

[251] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[252] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[253] UN CTED 2022 Trends Alert.

[254] RHIPTO, INTERPOL, and Global Initiative Against Transnational Organized Crime, "World Atlas of Illicit Flows" (2018).

© FATF-OECD 2025

8. Methods linked to criminal activities

257. At the level of the UN, States have expressed increasing concerns that terrorists can benefit from criminal activities as a source of financing or logistical support, through inter alia the trafficking in arms, persons, drugs, artefacts and cultural property, the illicit trade in natural resources and wildlife, kidnapping for ransom, extortion, robbery, as well as transnational organised crime at sea[255]. Previous FATF reports also identified various forms of links between criminal activity and TF for many terrorist organisations. In 2021, FATF noted that building links with organised crime enables EoRMT groups to generate revenue. It also provides opportunities to get access to restricted or illicit goods, such as weapons or forged documents, which allows the groups to increase their criminal activities[256].

258. In terms of funding their activities, terrorists are opportunistic and extremely adaptive to the conditions they operate in. The overlap between terrorism and organised crime further complicates counter-terrorism efforts, with some groups directly engaging in drug trafficking, human trafficking, and other illicit activities to diversify their income streams. In such scheme, terrorist organisations can either interact with organised crime groups at different stages of the criminal value chain, or act autonomously by replicating organised crime activities to generate profit. Others maintain an operational linkage, imposing taxes on transit routes or imposing facilitation fees, but not directly engaging in smuggling and trafficking activities. Terrorist organisations can also turn to organised crime groups as service providers, including for money laundering, smuggling, and weapon procurement.

259. The types of criminal activity and the nature of linkages vary considerably depending on regional and economic context, prevalent criminal activity and proximity to smuggling routes, as well as the degree of access terrorist may have to the resources they can exploit. Subsections below provide examples of linkages documented thus far, but this is not an exhaustive list, especially as these convergences are quite fluid.

8.1. Extortion, taxation-like activity, and coerced fees

260. Terrorist organisations often collaborate with local and regional criminal networks to raise and move funds deploying the use of threats or violence to extract money from businesses or individuals, which can then be funnelled to support terrorist activities. Extortion is one of the significant sources of funds for terrorist organisation. Taxation-like activity is as another method through which terrorist organisations, which control territory, resources, or economic activities, can generate revenue. This can involve the imposition of tax-like fees on local populations or businesses (including those operating with natural resources, agriculture or fishing), often under the guise of providing

[255] The United Nations Security Council has consistently recognized and expressed concern at the connection between transnational organised crime and terrorism in several of its resolutions, including resolutions 1373 (2001), 2462 (2019) and 2482 (2019). Furthermore, the General Assembly, in the Seventh review of the United Nations Global Strategy (GA 75/291) in 2021. In the Seventh review of the Global Counter-Terrorism Strategy, the General Assembly also took note of the nexus and encouraged Member States and international and regional organizations to enhance knowledge of and support initiatives to address, in the design and implementation of global, regional and national counter-terrorism strategies, the linkages between terrorism and transnational organised crime.

[256] FATF, Ethnically or Racially Motivated Terrorist Financing (2021).

© FATF-OECD 2025

protection or services to legitimise their activities, or as a form of coercion. Collections of fees or extortion take place at checkpoints in the form of so-called "road-taxes", or from businesses and locals located in areas both under and outside the group's control, including the diaspora for protection of their families and businesses. Extortion also happens at sea. In some contexts, extortion is used with kidnapping and coercion methods. This widespread use of extortion, coercive fee collection, and taxation-like practices by terrorist organisations has been corroborated by national delegations and further reinforced by private sector feedback, which consistently identifies these methods as key TF risks in areas where terrorist actors exert control.

261. Extortion or comprehensive "taxation" methods prevail as primary sources of income for terrorist groups in several parts of Africa (e.g., Al-Shabaab[257], JNIM), and in Yemen, where AQAP uses extortion of local business to pay for protection. This is also one of the predominant financing methods used by ISIL and its regional affiliates. The group still controls illegal commercial routes and taxes smugglers of weapons and narcotics and human, including in East and West Africa, Libya, and in Iraq and Syria. ISIL in Somalia has enhanced its extortion within the area of Bossaso focusing on businesses, exports and the shipping industry replicating Al-Shabaab's illicit taxation and extortion methodology to enhance the group's resource base, taxing some commercial, mining, trading, frankincense production and farming activity in Puntland[258].

262. The use of taxation-like methods by terrorist networks applies in several contexts as a tactic to generate revenue, usually in combination with other methods and criminal activities. When coupled with the threat of violence, terrorist groups have also used taxation as a tool of control over populations and to exert influence over territory. This has been a common method used by groups like Boko Haram, ADF[259], ASWJ[260] and Al-Shabaab[261]. Groups such as Al-Shabaab, ISWAP, and ASWJ have also used taxation to generate revenue for the provision of public services such as health care and education in the territories they control. This strategy further reinforces the influence they exert over local population.

[257] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[258] S/2024/556 , paragraph 35.

[259] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[260] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[261] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

263. In Eastern and Southern Africa, Al-Shabaab[262] is also known to have relied extensively on extortion to mobilise revenue for its operations. Controlling a large territory in Somalia, Al-Shabaab levies taxes on goods and businesses collected by a network of its "intelligence serves" (amniyat), with Mogadishu and southern Somalia remaining its biggest tax base. Al-Shabaab exploits the collection of zakat, using targeted lifestyle audits of wealthy businessmen. The group has divided its taxation system into distinct revenue streams for collection of taxes from vehicles, transported goods, farms and agricultural produce, and livestock sales. Al-Shabaab relies on the use of mobile money to levy taxes and receive extortion payments at checkpoints, and from traders importing goods, later transferring the funds to local domestic bank accounts. In 2016, the UN Monitoring Group on Somalia and Eritrea estimated that Al-Shabaab imposed a tax of USD 1,500 per truckload of sugar, with as many as 230 trucks passing through each week

264. In addition, terrorist groups may levy fees to allow criminal networks to operate as a form of license for their activities. In West Africa, ISWAP has been collecting various fees from petty offenders. For example, between August 2020 and March 2021 alone, ISWAP is reported to have earned approximately USD 65,000 from fines for non-severe offenses, which do not carry a death sentence, or which do not require amputation. In this context, they can establish legitimacy as providers of justice.

[262] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

Case study: Extortion of seasonal workers and real estate agents for TF purposes

In 2022, international terrorist organisation, which involved launching fundraising aid campaigns for the PKK[263]. Funds were collected from individuals who came from southeastern Türkiye to western Türkiye for seasonal work, taking 25% of their daily wages as a coercion fee. The organisation also charged real estate agents with a commission for the property selling and imposed it by threat. It has even been found that PKK forcibly made some real estate agents sell houses and pay a fee equivalent to 50% of the selling price of the property. In 2022, Türkiye uncovered a financing scheme supporting the PKK, through fundraising campaigns for the organisation. The scheme involved coercing individuals from southeastern Türkiye, who travelled to western regions for seasonal work, to contribute 25% of their daily wages. The organisation also extorted real estate agents, charging commissions on property sales under threat, with some agents forced to pay up to 50% of the sale price.

Funds were collected in cash, placed in yellow envelopes marked with serial numbers, and distributed to the PKK. Those who refused to pay the coercion fees were threatened. The money was regularly sent to border cities near PKK-controlled areas, where it was subsequently moved across borders to support PKK operations.

Source: MASAK (FIU), Türkiye.
Note: This case references an organisation under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). See: https://www.mfa.gov.tr/pkk.en.mfa

8.2. Kidnapping for ransom

265. KFR involves abducting individuals and demanding a ransom payment for their release. There is a persisting concern about the continued use of KFR operations by terrorist groups to generate revenue as well as to intimidate and exert influence and control over populations (distinct from KFR criminal purposes unrelated to terrorism). In fact, KFR is often referred to as a major element of terrorist strategies because it fuels insecurity and represents a highly profitable funding source. Payment of ransoms, which contravene UNSCR 2133 (2014), have significantly enhanced terrorist capability, resulting in loss of life. Given that ransoms are often paid secretly, exact numbers are difficult to establish but they likely add up to millions of dollars per year.

[263] Organisation under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). This applies for all references to PKK in the text box.

© FATF-OECD 2025

266. Nearly all terrorist networks operating in Africa, including Al-Shabaab[264], ADF[265], Boko Haram and ASWJ[266], use KFR as a means of raising revenue, often targeting foreign nationals and high-value local targets. In West and Central Africa, the example of payment of ransom of up to EUR 183 million for release of 80 hostages who were kidnapped in the Sahel indicates the lucrative nature of kidnapping as a revenue source for militant groups operating in Algeria, Mali, Mauritania, Nigeria and Niger. Al-Qaida affiliate JNIM is one such group that also rely heavily on kidnaping for ransom to extort funds and carry out abductions. ISWAP also relies on kidnappings to shore up its revenues, mainly humanitarian aid workers and government officials. Kidnappings have also been used to gain leverage and negotiate for prison exchange. For example, Boko Haram is notorious for using kidnapping as a bargain for the release of its own fighters.

267. There is a prevailing trend of raising revenue through a combination of methods where ransom payments are made either in cash or through hawala to avoid detection and tracing. Some jurisdictions also report on ISIS-related groups requesting payment to be processed through VAs. The demand for ransom can be exemplified from the capture of six Cuban doctors who were abducted by Al-Shabaab[267] for payment from the Kenyan government for their release. In DRC and Northern parts of Uganda, ADF[268] has also relied on abduction of individuals, including children, for ransom to extort payments from the local populations. Further in Mozambique, authorities have reported incidences where villagers have been kidnapped by ASWJ[269] terror group mainly at night and demands made for large sums of ransom payments. At the same time, Boko Haram demands payment in form of 40 herds of cattle for the return of each of the kidnapped women. Cattle as a commodity for settlement, rather than cash, may be indicative of Boko Haram's financial

[264] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[265] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[266] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[267] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[268] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[269] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

management strategy where they hold the cattle as a means of storage and later sell the same for higher value.

268. There is also an emerging trend where terrorist groups work in concert with criminal gangs to engage in kidnapping as a commercial activity. In this context, there is no demand for ransom, but the terrorist group "sells" the kidnap victims to other criminal networks. For example, Boko Haram mainly involves kidnapping of women and girls for purposes of selling the victims into slavery or for suicide attacks. In some instances, criminal groups will engage in kidnapping on their own frolic but later sell the hostages for cash to the terrorist organisations who will in turn demand premium ransom for their release.

269. KFR is also a known source of funding for some Taliban-associated groups operating in Pakistan and Afghanistan. AQAP relies heavily on KFR and is noted to have an abduction cell that increased KFR operations in Yemen in 2023 and 2024, especially targeting foreign employees of international organisations. One example reported in 2021 of a ransom case involving a kidnapping in northern Iraq was reported to have netted almost USD 1 million to ISIL[270]. Until recently, Abu Sayyaf Group (ASG) former leader was notorious for masterminding maritime kidnap-for-ransom operations in South-East Asia.

270. Other regional or subregional armed groups that are designated as terrorist on national levels are also known to widely resort to KFR in Latin America (e.g., Maras Salvatrucha[271] in El Salvador).

271. In some situations, elements of human trafficking and KFR are intertwined. There are documented cases where the payment of a ransom by the family of abducted persons (notably Yazidi women and children) to ISIL was done directly or through smugglers who act as "middlemen" and demand extra fees to execute the rescue operation. The amount paid by the family represents a direct compensation for the operation, since the smugglers essentially "steal the [individuals] from ISIL"[272]. The abductions perpetrated by Boko Haram and ISWAP in Nigeria also blur the distinction between human trafficking and KFR. The FATF has also acknowledged the use of human trafficking by terrorists as "an occasion to secure ransom payments".

8.3. Human trafficking and migrant smuggling

272. Human trafficking continues to be one of the most profitable activities of organised crime and is perceived by the perpetrators, including armed groups and terrorists, as a high-profit—yet low-risk—criminal activity. Trafficked persons are exploited as merchandise to be sold and re-sold; to secure ransom and rescue payments[273]; and as instruments to perform servitude roles. UNSC resolutions repeatedly called on Member States to improve efforts and take decisive action to identify cases of trafficking in persons

[270] UN 1267 Monitoring Team, 30th Report t of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610(2021) concerning ISIL (ISIL), Al-Qaida and associated individuals and entities.

[271] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[272] UN CTED Report on Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing (2019).

[273] See sub-section on KFR. See also UN CTED report on Towards meaningful accountability for sexual and gender-based violence linked to terrorism (2023), page 9.

© FATF-OECD 2025

that finance terrorism with a view to holding those responsible accountable[274]. Yet, there continues to be near-complete impunity for human trafficking and sexual violence crimes perpetrated in a terrorism context[275].

273. In 2016, the UN Secretary-General reported that ISIL, Boko Haram, Al-Shabaab[276] and others are using trafficking and sexual violence as weapons of terror and an important source of revenue[277]. The FATF has also noted that there are "indications that human trafficking may be source of income for terrorist groups, particularly those that control territory" [278]. In 2019, as mentioned under Section 1, the example of systematic sale of Yazidi women by ISIL fighters represents the most significant known instance of the use of sexual slavery to generate revenue (i.e. of the 'human trafficking/TF nexus')[279].

274. Human trafficking constitutes a highly opportunistic source of financing for terrorists, who can profit from their victims in many ways and exploit them as "reusable commodities". Whereas the ISIL slave trade required some investment (including for payment of logistics and transportation) and considerable organisation, other forms of abuse enable the victims to be directly exploited without any additional "expense"[280].

275. The link between TF and migrant smuggling can manifest in several ways[281]. There is ample evidence of terrorists receiving money from smugglers along certain migration routes in the form of 'tolls' for safe passage through the territory they control. In that sense, the main geographical area where terrorist organisations are considered to have obtained profits from migrant smuggling is in Africa, where some regions are currently under terrorist groups' control. According to the 1267 Monitoring Team, ISIL still controls illegal activities of smugglers of humans, including in East and West Africa, Libya, and in Iraq and Syria.

276. There may also be terrorism-related risks, where migrant smuggling networks help conceal travel of their members, such as returning or relocating FTFs. In this regard, there has been a noticeable trend of larger sums being sent to returning FTFs, often used for handover to terrorist groups before departure, or to pay traffickers and smugglers[282]. In the past five years, funds have been raised and used to smuggle ISIL affiliates and/or their

[274] E.g., Resolutions 2331 (2016) and 2388 (2017). The Council has highlighted the key role of financial intelligence units through analysing and detecting transactions that may be linked to human trafficking, as well as in disseminating guidelines and risk indicators.

[275] UN CTED's 2021 Global Implementation Survey (S/2021/972).

[276] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[277] United Nations, Secretary-General, seventy-first session, 7847th meeting of the Security Council, 20 December 2016, S/PV.7847, page 3

[278] FATF and Asia-Pacific Group joint report on Financial Flows from Human Trafficking (2018), paragraph 41

[279] UN CTED Report on the Nexus Between HT, Terrorism, and TF, 2019, paragraph 61

[280] UN CTED Report on the Nexus Between HT, Terrorism, and TF, 2019, www.un.org/securitycouncil/ctc

[281] See the FATF 2022 report on ML/TF risks arising from migrant smuggling. See also examples in the UN CTED Report on Identifying and Exploring the Nexus Between Human Trafficking, Terrorism, and Terrorism Financing (2019).

[282] UN CTED 2024 Trends Tracker

© FATF-OECD 2025

family members from camps and prisons[283]. There are consistent reports of individuals who have been smuggled out of the camps for a payment of approximately USD 2,000.

277. In 2022, the FAFT noted that in Africa, authorities detected cases where armed terrorist groups obtained funding from migrant smuggling[284]. In these cases, terrorists or terrorist groups are not directly involved in the trafficking of migrants (a phenomenon that has not been observed). However, because of the territorial control exercised by certain terrorist groups in Africa, or the control of transport lines or nodes in migratory routes, migrant smugglers, or migrants themselves can be required to pay "tolls" for passage or compensation in exchange for security. Similar cases have been seen in Libya and Mali in particular. In addition, migratory routes in parts of Africa coincide with areas where terrorist organisations have control or influence over territory, including in Burkina Faso, and Niger as well as Mali, giving rise to these risks.

278. The ongoing internal turmoil, instability and conflict affecting areas in Syria, Iraq, and Afghanistan, is resulting in migration to Türkiye and Europe, also creating a source of income for terrorist organisations operating in Syria and Iraq. Migrant smuggling activities are sometimes carried out under the control of terrorist organisations, together with the networks they have created in the regions close to the Turkish borders. There are also links to organised criminal groups operating in the region.

279. There is limited evidence on systematic migrant smuggling-related cooperation between criminals and terrorists in the EU. However, EU member states continue to highlight the risk of abuse of migration flows by terrorist groups and returnees, along with related screening challenges. Those that did return included an indicative case of two ISIL members who entered Spain by boat from North Africa, receiving logistical support from networks in Morocco. There is therefore the potential for networks in North African to facilitate returning FTFs, such as from Libya, either directly to South European, or via Morocco into Europe.

280. No information has been reported in relation to links between TF and migrant smuggling in relation to the other significant migrant smuggling routes in North and South America and in Southeast Asia.

8.4. Trafficking, smuggling of goods, and illicit trade

281. Smuggling is a significant component of revenue generation for terrorist groups. Terrorist organisations with territorial control have been known to benefit from ensuring the safety and protection of commercial enterprises in the controlled territory, as well as organising illegal routes for the transfer of smuggled goods. As mentioned above, the vulnerability created by porous borders, in proximity to ongoing conflicts and limited government controls in remote areas, provides a conducive environment that allows movement of goods across borders under the control of armed groups and terrorist organisations. In Africa, it has become a continuing trend for terrorist groups to establish smuggling routes for goods, minerals, timber, fish, weapons, livestock, and other contraband.

[283] UN CTED 2024 Trends Tracker

[284] FATF Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling (2022)

© FATF-OECD 2025

282. For example, in DRC, ADF[285] has been noted to rely on smuggling of minerals and timber, at times relying on the services of other arm groups who control smuggling corridors to ship the minerals and timber to neighbouring countries[286]. In Somalia, Al-Shabaab[287] has been involved in sugar smuggling across the Kenyan-Somalia border[288]. Additionally, Al-Shabaab[289] has also been involved in the illicit trade in weapons between Yemen and the Horn of Africa as well as charcoal smuggling[290] to the Middle East, exploiting the sea routes to facilitate small-scale shipments via speedboats across the Gulf of Aden. ASWJ[291] frequently engages in cross-border smuggling, utilising Mozambique's porous borders, and integrates licit and illicit supply chains involving motorcycles, fuel, drugs, tobacco, and medicine. AQ affiliate in the lands of AQIM receives funds from weapons and drugs smuggling, illegal migration in the Sahara-Sahel zone of Africa. In West and Central Africa, Boko Haram and ISWAP use smuggling routes to transport not only goods but also fighters and weapons. Boko Haram engages in diverse informal trading activities to fund its operations, including the illegal trade in fuel, scrap metal, and aluminium[292]. Overall, the most common items for smuggling include fuel, food, weapons, and other contraband. There are also instances where terrorist organisations operating in West and the Horn of Africa have collaborated with petty criminals for a common pursuit of smuggling of goods and trafficking in drugs.

283. The ISIL al-Karrar Office in Somalia collaborates with organised crime networks, pirates, and even rival terrorist groups like Al-Shabaab[293] and AQAP to smuggle illicit goods. AQAP receives income from illegal sales of weapons and petrochemical products.

---

[285] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[286] Group of Experts on DRC, S/2024/432.

[287] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[288] Sweet Secrets: Sugar Smuggling and State Formation in the Kenya—Somalia Borderlands, 2017

[289] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[290] Exploitation of natural resources and terrorism, UNODC Sherloc. www.sherloc.unodc.org

[291] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[292] S/2025/71/Rev.1, paragraph 105.

[293] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

8.5. Drug trafficking

284. Drugs trafficking is a major source of revenue for certain terrorist and insurgent groups that are involved in the illegal drug trade, controlling commercial routes and taxing narcotic smugglers, a tactic observed with notable frequency. Furthermore, these groups may be directly involved in the production, processing and trafficking of drugs. Some terrorist groups have been reported to tax transnational drug shipments and collect fees from drug traders.

285. ISIL and its regional affiliates are involved in the illegal drug trade, notably in Captagon, controlling commercial routes and taxing narcotic smugglers. There have been reports of links between drug trafficking and TF in West Africa among groups such as Boko Haram and other affiliates organisations with ISIL and AQ[294]. Moreover, there is evidence that proceeds from drug trafficking have been used to support terrorist operations in the Sahel[295], although the trade and consumption of drugs is not common in areas where Al-Shabaab[296] operates due to religious and cultural sensitivities.

286. Research indicates that Northern Mali is a lucrative route for the global narcotics trade, with local traffickers working with powerful cartels in Latin America to traffic drugs through the country's north into Algeria and onto the European markets. If the Islamic State of Iraq can successfully seize these lucrative trafficking routes, it could become a significant revenue generator for the IS organisation and, with the help of Maktab al-Furqan, could funnel some of this revenue to finance global attacks by other branches, such as ISIL-K[297].

8.6. Illicit arms trade

287. The UNSC expressed grave concern that terrorists benefit from organised crime as a source of financing or logistical support through the trafficking of arms and urged countries to implement several legislative and operational measures in this regard. In 2021, the FATF issued a non-public report examining how IAT relates to TF. The risk of terrorist groups raising funds from IAT has also been noted by several countries in regular FATF updates on ISIL, AQ and affiliates financing.

288. As clarified by the FATF[298], TF through IAT implies that a terrorist actor has already acquired the arm, whether legally or illicitly, and uses it to generate revenue by selling it to another party. Though limited, public reporting suggests that terrorist organisations, particularly those controlling territory, raise funds by engaging directly in arms trafficking.

---

[294] Statistics Suggest Sharp Increase in Sahel Drug Trafficking: Africa Defence Forum, 2024.

[295] UNODC report on Drug Trafficking in the Sahel (2024).

[296] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[297] Global Network on Extremism & Technology, Combating Islamic State Finance: West Africa and the Sahel, Insight by Adam Rousselle, February 2025.

[298] FATF Confidential Report on Tackling Illicit Arms Trafficking and Terrorist Financing, Outcomes FATF Plenary, 22, 24 and 25 February 2021

© FATF-OECD 2025

For example, Al-Shabaab[299] may be selling their arms to businessmen and use funds raised from these deals to pay to its fighters.

289. Terrorist groups also see illicit arms as a commodity that can be exchanged with other terrorist groups or other armed actors for goods. Al-Shabaab[300] fighters may be smuggling arms through the borders to supply local civilians who then barter or sell stolen livestock in exchange for these arms. Lone actors and small terrorist cells, on the other hand, appear to be on the demand side of the IAT.

290. This risk appears to be more material for regions with higher terrorist threats and suffering from conflict or with recent experience of conflict, as it requires a certain degree of organisation from a terrorist group, a permissive environment, and a surplus of arms supply for the terrorist group to get funding through this IAT. For example, the 2013 joint FATF/GIABA report highlighted IAT to be a source of financing for Boko Haram.

291. Although not detailed, FATF 2021 reporting suggests that groups can still sell previously procured small arms and light weapons (SALWs) to replenish their budgets. Given the array of techniques to move funds that terrorists have been known to use, (e.g., cash couriers, hawala networks), the identification and investigation of such cases remains extremely challenging for authorities. In addition, IAT would likely occur in areas either controlled by a terrorist group or where the group has a significant presence or influence, is what limits visibility over the deals by competent authorities. However, investigation of a crime committed with the use of an illicit arm can often lead to a discovery of the IAT chain, tracing the smuggled arms to the conflict zone.

8.7. Illicit trade and trafficking of cultural property

292. The UNSC has repeatedly identified the trafficking of cultural objects as a source of TF used by ISIL, Al-Nusrah Front (ANF), and other individuals, groups, undertakings and entities associated with AQ[301]. The FATF has noted the exploitation of antiquities by ISIL, AQ and its affiliates since 2016 during its regular monitoring of the financing methods of these groups. In 2023, the FATF published a dedicated report on Money Laundering and Terrorist Financing Risks in the Art and Antiquities Markets[302].

293. Research on these linkages has primarily interested certain regions and countries, such as Syria and Iraq, or Afghanistan, over others which have seen an increase in terrorist activities in recent years, including within the African continent[303]. Therefore, the understanding of the scale of proceeds generated through trafficking of cultural property from such regions and their use for TF purposes remains limited.

---

[299] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[300] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[301] See*, inter alia*, resolution 2199 (2015), 2253 (2015), 2347 (2017).

[302] FATF, Money Laundering Terrorist Financing Art Antiquities Market (2023)

[303] See, e.g., UN CTED Threats and Trends: The Traffic and Illicit Trade of Cultural Property for Terrorist Purposes (2022).

© FATF-OECD 2025

294. Terrorist groups institutionalised the looting and illicit sale of artefacts as an important source of revenue, through a system of smuggling and taxation-like tactics. In areas under control of certain terrorist groups, considerable resources have been dedicated by them to the excavation, looting and sale of antiquities, and made it an important source of revenue[304]. While the precise amount is still unknown, the most conservative estimates point to tens of millions of dollars stemming from these activities alone.

295. According to UNICRI's 2024 report[305], antiquities for sale in local markets across Iraq and Syria were seen from 2019 onwards. Some of the antiquities were traded by ISIL fighters and facilitators through their network of local contacts. There have also been reports from some sources about ISIL members and contacts trying to sell antiquities in Iraq and Syria to raise funds to pay human smugglers to get them out of the conflict zone. Others claim that ISIL's mid-level commanders and local leadership have stockpiled antiquities in mountains and desert hide-outs since 2017 in anticipation of the group's demise.

296. While today groups like ISIL may have lost territory in Syria and Iraq, these same techniques are being replicated by their affiliates in other regions of the world, and the smuggling routes being used and converging with other illicit flows of transnational organised crime[306].

297. In this regard, the FATF has noted that transnational crime groups have been observed cooperating with terrorist groups to acquire cultural objects, then using their networks to smuggle these items out of conflict areas, and into destination markets for sale[307]. Small criminal groups can operate under the umbrella of a larger criminal organisation to help facilitate the supply chain for smuggled or stolen cultural objects. In such cases, members of these groups play distinct roles, such as excavators, mediators, domestic vendors, exporters, and sellers of the antiquities through auction houses and dealers and to private buyers. Certain complicit dealers are sometimes closely engaged in these supply chains. These dealers, either cooperating with organised criminal groups or through direct involvement in these groups, participate in the smuggling or sales of looted or excavated cultural objects. Some of them may also provide false documentation or invoices to facilitate the smuggling process.

298. In addition to traditional venues and market participants, social media platforms have been used to connect, advertise, and sell looted cultural objects[308]. Algorithms are used to connect members, drive content choice, and help facilitate connections between

[304] ISIL (ISIL)'s plundering and destruction of cultural heritage in the territory they held until 2019 had two objectives: first to gain profit by selling culture as an illicit activity that proved to be a reliable source of funding; and second, to destroy culture and rewrite history according to the narrative of its ideology (this action was termed by UNESCO as 'cultural cleansing') – see UNICRI 2024 Report on Cultural Heritage Smuggling and the Nexus with Terrorism (www.unicri.it). FATF noted in its 2023 Report that ISIL directly benefited from the excavation, looting, and trafficking of cultural objects, including by selling it to third parties, as well as from taxing non-ISIL members for the excavation, looting, and smuggling of cultural objects on territory that it controls.

[305] UNICRI report on Cultural Heritage Smuggling and the Nexus with Terrorism (2004).

[306] See FATF 2023 report highlighting the role of transnational organised crime groups cooperating with terrorist groups to acquire and smuggles cultural objects.

[307] FATF, Money Laundering and Terrorist-Financing in the Art and Antiquities Market (2023)

[308] Op. Cit. See also Al-Azm, A., & Paul, K. A. (2019). "Facebook's black market in antiquities: Trafficking, terrorism, and war crimes"—available at www.atharproject.org

© FATF-OECD 2025

looters, facilitators, buyers, and sellers. Private groups on social media sites and group chats on messaging applications with hundreds of thousands of members can keep information out of the hands of law enforcement using privacy settings and encryption.

299. Although no relevant cases were identified, the FATF also noted that terrorist groups could also create counterfeit antiquities themselves to generate funds through these markets. As with other criminals, terrorists and their facilitators could also manipulate the value of cultural objects, either by inflating the price of counterfeit objects or by listing authentic antiquities as inexpensive modern copies to evade export regulations.

300. Successful cases[309]:

- Seizure of an extraordinarily well-preserved statue looted from the ancient city of Palmyra thanks to the Antiquities Trafficking Unit of the Manhattan District Attorney's Office.
- Efforts of the Spanish National Police, with the support of Europol, that led to the dismantling of a network of intermediaries trafficking antiquities from sites in Libya.
- 2022 reiteration of Operation Pandora—a joint pan-European law enforcement operation—that led to 60 arrests and the seizure of over 11,000 cultural objects.

8.8. Theft, robbery, and petty crime

301. Robberies (including banks, commercial enterprises, ships, fisheries and farms, hospital, and health centres, or individual and trucks carrying various goods) have also been identified as a viable option for terrorist organisations to access large sums of money. In West Africa, groups such as Boko Haram actively participate in robbery and looting activities to finance themselves and obtain the necessary goods to survive (attacking vessels, police stations, army barracks, looting small villages and farms and attacking villages during market days to get cash and food items). AQAP generated income from robberies (including banks and exchange offices). Furthermore, ADF[310] funds its operations through hijacking traders, stealing the minerals from them, and smuggling the same to market towns outside the country. Pakistan reports on TTP conducting bank robbery and looting on bank vans. In 2021, FATF also noted robberies as a source of funding for EoRMT groups.

302. Whereas large-scale criminal activities aiming at TF are mostly to be seen from organisations displaying strong territorial presence, low intensity criminality can be observed in self-financing contexts. Local small cells' members and lone terrorist actors, including FTFs, can turn to petty crime to generate small amount. Such activities can include retail drug dealing, small-scale robbery, scams, tax or social benefits fraud, and the sale of counterfeit goods.

---

[309] See FATF Money Laundering and Terrorist-Financing in the Art and Antiquities Market (2023) for more cases.

[310] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

9. Methods based on legally generated revenue

9.1. Self-financing from licit sources, including savings, salaries, social benefits, family support, and loans

303. Self-financing from licit sources is considered as the main fundraising method used by small-cell members and isolated individuals, including in contexts of ethnically and racially motivated terrorism. Individuals are known to often rely on income revenue and personal savings to finance their travel to conflict-zone, to conduct an attack in their country of residence or in neighbouring countries, to acquire propaganda material, or to transfer small donations to larger terrorist networks. As previously noted, self-financing from licit sources was already a major funding method for FTFs during the period when departures to conflict zones were prevalent, and it remains so today—both in supporting FTFs who remain in conflict areas and in financing their return.

304. Even though FTFs departure to theatres of operations considerably declined with the weakening of ISIL in Syria and Iraq, self-financing by small-cells members or lone actors is likely to remain a predominant concern. Many jurisdictions which used to be confronted with FTF departure indeed consider they are now mainly exposed to endogenous threats from self-radicalised individuals. The latter also mostly rely on self-financing, insofar as they turn to low-cost modus operandi involving less firearms but rather bladed weapons or cars.

305. Self-financing first takes place through personal revenue of individuals: work income, savings, or social benefits. Cases were also documented of individuals selling personal items prior to joining a terrorist organisation in a conflict-area, or to conducting an endogenous terrorist attack. Among most common occupations through which terrorist individuals generate revenues, jurisdictions mention self-employment and micro-enterprises, particularly in the construction and public works, as well as private security sectors. Regarding social benefits, some delegations observe a steady dependence of terrorist individuals over the past ten years, and a growing capacity to cheat on tax returns to perceive more benefits.

Case study: Funding a terrorist act through the selling of personal items

In 2019, a terrorist attack took place in Northern Lebanon and resulted in the death of law enforcement officers, army personnel and the injury of several civilians. The terrorist, known to be affiliated with ISIL, opened fire on army personnel, and detonated an explosive vest after a pursuit and confrontation with law enforcement officers. The Lebanese LEA determines that the terrorist did not receive instructions from ISIL leaders but instead committed what was described as a "lone wolf" operation after having served time in jail for joining ISIL in Syria. İnvestigations revealed that the terrorist sold his house furniture and used the proceeds to self-finance his attack. Proceeds in cash for approximately USD 1000 were used to buy ammunition.

Source: Special Investigation Commission, Lebanon[311]

[311] For further information see: www.bbc.com

© FATF-OECD 2025

306. Besides their personal revenues, individual terrorists can also rely on financial supports from their relatives, friends or community members, who knowingly and willingly or unwillingly end up supporting a terrorist activity. In additions to being mobilised prior to an operation or a travel to conflict zone, family support is also likely to be observed in the case of FTF remaining in conflict-area, especially those under detention.

307. Microfinancing of licit origin is intrinsically hard to detect and to obstruct, for it does not convey any particularity on its own that can catch the attention of regulated private actors or authorities. Therefore, jurisdictions exposed to this type of TF risk can opt for targeted financial sanctions consisting of freezing all resources and assets owned or controlled by individual known for their terrorist activity. While targeted sanctions are enforced under UNSCR 1267 at multilateral level, the low-scale dimension of TF threats from small cells and individual terrorists require local intelligence and investigation to consider even the weakest signals. This confirms the relevance of sanction regimes taken at domestic or regional level under UNSCR 1373, in full compliance with international law including human rights and international humanitarian law, as well as of submitting designation proposals of FTFs and their facilitators and financiers to the UNSC Committee pursuant to resolutions 1267 (1999), 1989 (2011), and 2253 (2015)[312].

308. An ongoing challenge though remains in cases when individual terrorists rely on third parties' resources (cash, bank accounts, legal entities) on which they informally exert control or ultimate beneficial ownership, through tacit understanding among actors. Authorities should thus be encouraged to conduct analyses of suspects' financial environment in order to detect potential circumvention of targeted financial sanctions.

[312] UNSC resolution 2396 (2017), OP42.

© FATF-OECD 2025

Case study: Criminal investigation on self-financing of terrorism

In 2019, the Dutch Fiscal Information and Investigation Service and the Public Prosecution Service initiated an investigation against a person suspected of raising money for ISIL-female Foreign Terrorist Fighters (FTFs) in detention camps in Syria.

The investigation started after publication of news articles in two different Dutch newspapers; the "NRC" and "De Telegraaf" and an interview with the subject in newspaper "de Volkskrant". In these publications, it was mentioned that the subject, together with another person, raised money for female FTFs.

The following investigation, consisting among other things of wire taps and search warrants, led to the conclusion that over a period of two years, the suspect made money available to many women and children who were staying in detention camps in Syria. Initially for food and goods, later for 'escapes' of women and their children from the camps. He did this by collecting funds in cash and moving them through hawala (considered as an underground banking system in the Netherlands) to the ISIL Syrian-based camps. The suspect played a guiding and essential role in this: he gave orders concerning which women had to be picked up, organised the smuggling, and arranged accommodations. These were mainly Dutch women who had previously travelled to Syria, stayed there for a long time and were (or were) married to ISIS fighters/employees.

By his actions, the suspect took the risk that the money would (indirectly) end up with ISIS and be used for terrorist purposes. For this reason, the suspect was convicted for TF and violation of the sanctions act. In addition, the suspect, together with another person, filed a false VAT return and falsified an administration by including a false invoice in it.

The suspect was sentenced to a prison sentence of 30 months, minus pre-trial detention.

Source: Netherlands National Prosecution Service. See: www.uitspraken.rechtspraak.nl.

9.2. Formal economic activities (including investments, business activities, merchandising, and events)

309. Terrorist organisations can set-up formal revenue-generating activities to finance their operations. This method differs from the one based on informal activities as we are here focusing on terrorist organisations investing in formally declared economic activities. It also differs from methods based on the abuse of legal entities as in the present section companies are used to derive profit from an actual activity, and not only as an administrative front to hide beneficial owners, convey funding or emit invoices.

310. As this requires more administrative and economic know-how and allows to generate and/or launder significant amount of money, methodologies based on formal businesses are mostly observed in contexts where transnational and national groups are operating. Still, some specific revenue generating activities, like events or training organisation, are considered as trademarks of EoRMT groups.

© FATF-OECD 2025

311. Large terrorist organisations operating in multiple jurisdictions are known for controlling numerous local businesses in various jurisdictions, including in countries neighbouring their operations. Local shops can at the same time serve as front office for collectors to manage fundings aiming at financing terrorist operations, and as revenue generating structures.

312. Formal economic activities are also frequently reported when dealing with terrorist organisations operating in a limited geography. The Foundation for Defence and Democracies reported on the Haqqani Network[313] raising funds in various jurisdictions through supported conducting businesses in real estate or construction sectors[314].

313. Overall, Europol insists on various terrorist organisations investing in cash intensive businesses, such as construction, restaurant, cars and heavy machineries dealers, telecommunications companies, MSBs, and precious metals.

314. Delegations also report cases of foreign companies establishing in their jurisdiction to raise and accumulate funds on behalf of foreign territory-controlling terrorist organisations. These companies can operate as online stores, either via their own website or their respective online merchant profiles and are mostly active in the food processing and food businesses including small bakeries and online animal food shops.

315. Besides representing a source of revenue, investment in legitimate companies can in rarer cases be used as a storing mechanism, as it was reported by several delegations. Al-Shabaab[315] is estimated to spend about 70% of its revenues of operations and approximately 30% on investments[316]. The ability of terrorist groups such as Al-Shabaab to invest in sectors such as real estate and or health sector—not only within Somalia but also in other States exemplifies the risk that terrorist organisations with significant financial resources employ sophisticated schemes to invest in non-financial sectors abroad.

316. Specific lawful economic activities involving smaller sums are particularly associated with the financing of EoRMT. These activities may include membership fees to associations, the sale of merchandise such as clothing, stickers, and pins, the distribution of ideological materials including books and music, as well as the organisation of concerts and other events. South Africa also notes the offer of specialised training as a common method to raise funds for EoRMT groups. The type of training deals with self-defence and personal protection training and includes anti-hijacking and training to prevent farm attacks and house robberies. Individuals attending the training pay it and will also purchase uniforms, T-shirts, and caps.

317. Publishing houses, bookstores, and royalties from bookstores (made online or in physical stores) are revenue generating activities that also serve propaganda objective and that can be observed in various contexts and serving diverse ideologies.

---

313 Organisation designated under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

314 A Network of Possibilities: How the Haqqani Network Changed the Face of Global Terrorism Forever – Georgetown Security Studies Review

315 Organisation designated under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

316 UN 1267 Monitoring Team, S/2025/71/Rev.1, paragraph 42

© FATF-OECD 2025

10. Methods based on the abuse of legal entities

318. Corporate vehicles[317] such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements can be vulnerable to TF exploitation, as their involvement in a wide range of commercial and entrepreneurial activities[318] makes them attractive tools for circumventing CFT measures and facilitating other illicit purposes.

319. Delegations reported primarily the use of shell companies, the creation of structure of enterprises in multiple jurisdictions and investment on multilayer schemes on big and small business for TF purposes. As mentioned before, given the disruption activities competent authorities have employed, terrorist organisations and individuals are shifting form traditional methods to more complex schemes to raise, move, store, and spend their funds. Their professionalisation in the creation of multiple layers of interconnected business and the employment of investment strategies is an area of concern where TF indicators should continue to be developed for an early detection.

10.1. Use of front and shell companies

320. Several delegations mentioned the use by terrorist companies of front and shell companies to move funds with increased opacity. Methods based on front and shell companies differ from the ones based on formal economic activities, as they don't rely on legal persons to generate revenue through an actual economic activity, but only use the administrative opportunities offered by the legal person: emitting invoices, opening bank accounts, and operating transfers. There can also be schemes where companies with licit activities are used as front for TF purpose. In those occasions, licit and illicit funds are mixed, making detection even harder.

321. Those methods can pursue two aims: moving funds internationally through the regulated financial system, as the legal person allows to hide identities of beneficial owners; or to launder funds from illicit resources to ultimately invest them in formal businesses. In both cases, schemes are likely to involve opening bank accounts and conducting wire-transfers.

322. When setting up such schemes, terrorist organisations can exploit vulnerabilities offered by weak regulatory framework, as well as vulnerabilities emerging from varying regulatory standards from one jurisdiction to the other, as well as shortcomings in international cooperation, making it harder to detect fraudulent transactions operated between two legal persons located in different jurisdictions.

323. This method is mainly observed from organisations with transnational dimension and sufficient structuration. Several delegations reported on Hezbollah's military branch[319] relying on a front and shell companies operating across multiple jurisdictions to move funds internationally. The same has also been documented regarding ISIS. At

[317] This paper uses the term corporate vehicles to mean legal persons and legal arrangements, as defined in the glossary of the FATF Recommendations.

[318] FATF Guidance on Beneficial Ownership Legal Persons (2024)

[319] Organisation under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

© FATF-OECD 2025

regional level, several jurisdictions reported on ADF[320], Ansar al-Sunna, ASWJ[321] and Al-Shabaab[322] also relying on front and shell companies to move fundings. More specifically, jurisdictions have observed an emerging trend where Al-Shabaab use front and shell companies to invest in cash-intensive businesses, such as filling stations and transportation sectors[323] while the use of currency exchange businesses by terrorist groups to launder funds has also been noted, in particular in the Lake Chad basin region[324]. Hamas[325] is reported using front and shell companies to launder funds collected in cash as well.

324. Relying on front and shell companies requires some legal and administrative know-how, and many delegations which reported such cases indicated those schemes were rare and complex. However, as methods based on front and shell companies are already widely spread in the field of ML, any further convergence between organised crime and TF could result in such schemes becoming more common.

10.2. Abuse of non-profit organisations

325. As repeatedly recognised by both the FATF and the UN, NPOs play a vital role globally, both economically and socially. FATF's functional definition of NPOs focuses on their role of raising or disbursing funds. NPOs are at varying degrees of TF risks abuse by virtue of their types, activities or characteristics with the majority of them representing low TF risks[326]. Over the last decade, the FATF has undertaken extensive work on preventing the abuse of NPOs for TF while being mindful of potential unintended consequences and ensuring adequate human rights diligence.

326. In 2023, FATF noted that in rare cases, NPOs continue to be misused and exploited by terrorists through a variety of means[327]. Terrorists and terrorist organisations may seek to exploit NPOs to raise and move funds, to provide logistical support, to encourage

[320] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[321] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ASWJ is also monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[322] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[323] National TF Risk Assessment Report Kenya (2023)

[324] S/2025/71/Rev.1, paragraph 105

[325] Organisation designated under a supranational or national designation regime established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[326] Interpretative Note to Recommendation 8, paragraph 6

[327] The FATF report on Risk of terrorist abuse in Non-profit Organisations (2014) identified five types of abuse: (i) diversion of donations through affiliated individuals to terrorist organisations; (ii) exploitation of some NPO authorities for the sake of a terrorist organisation; (iii) abuse of programming/program delivery to support the terrorist organisation; (iv) support for recruitment into terrorist organisations; (v) and the creation of 'false representation and sham NPOs' through misrepresentation/fraud.

© FATF-OECD 2025

terrorist recruitment, to provide a veil of legitimacy, or otherwise support terrorist organisations and operations. In 2024, the Egmont Group identified the following six methods prevalent in the abuse of NPOs for TF purposes: diversion of funds; affiliation with a terrorist entity; abuse of NPO programs; providing support for recruitment; false representation; and fundraising through social media[328].

327. Both the FATF and the Egmont Group have signalled that in terms of activities, NPOs that are engaged in providing humanitarian services and/or operating in unstable high-risk environments (abroad-where fund or goods might be abused at the point of distribution by the partner organisations; domestically- when operating within a population that is actively targeted by a terrorist organisation for support and cover) are the most vulnerable to TF abuse[329], most frequently happening without their knowledge. Legitimate NPOs operating in foreign jurisdictions are at risk of having their funds or goods abused at the point of distribution by the charity or partner organisations. Similarly, NPOs that operate domestically, within a population that is actively targeted by a terrorist movement for support and cover, are also exposed to TF risks. This is because resources generated locally may be transferred internationally to support terrorism if the organisation does not exercise direction and control over the end-use of its resources. In addition, unregistered NPOs are overall highly vulnerable to TF activity as they are subject from minimal to no oversight, very little is known about their operations, and they are less aware of TF risks and available means to mitigate them.

328. Overall, NPOs operating in high-risk jurisdictions tend to be most exposed to TF risks when they are subject to minimal or no oversight. Unregistered NPOs are overall highly vulnerable to TF activity as very little is known about their operations, and they are less aware of TF risks and available means to mitigate them. Conversely, some jurisdictions have adopted effective risk-based mitigation strategies by supporting NPOs operating in high-risk areas to develop robust internal due diligence procedures. Risk-based measures[330] have also been applied to NPOs that benefit from public funding or exceed a certain size, ensuring proportionate oversight aligned with their risk exposure.

329. NPOs operating in high-risk areas can also face higher exposure to TF risks when they cannot rely on regulated financial services to conduct their operations and must turn to informal financial channels which involve weaker or no due diligence processes, and lesser traceability.

330. According to the Egmont Group, there may also be a heightened ML/TF risk associated with religious organisations, particularly religious NPOs operating in environments or within populations that terrorist entities actively target. For example, and as referenced in several sections above, groups like Al-Qaida and ISIL exploit the charitable principle of zakat to raise finance from communities around the globe[331].

---

[328] Egmont Group Report on FIU's Role in the Fight Against the Abuse of NPOs for Terrorist Financing Activities, public summary (2024)

[329] FATF best practices on Combating the Terrorist Financing Abuse of Non-Profit Organisations(2023); FATF Terrorist Financing Risk Assessment Guidance (2019); and FATF report on Risk of Terrorist Abuse in Non-Profit Organisations (2014)

[330] FATF Interpretative Note to Recommendation 8, A (4): It is also important for such measures to be implemented in a manner which respects countries' obligations under the Charted of the United Nations and international law, in particular international human rights, international refugee law and international humanitarian law. See also UNSCR 2462(2019) paragraphs 6 and 13 and UNSCR 2664(2022) para 1.

[331] Op. Cit.

© FATF-OECD 2025

331. In a different scenario, sham NPOs are established or registered knowingly for the purpose of TF and used multifunctionally to raise, store, and move funds, commonly under false charitable pretexts. For example, in East Asia, JeM, and Lashkar-e-Tayyiba (LeT) both associated with AQ, were reported to abuse humanitarian assistance donation programs using sham NPOs to divert funds and finance operational activities, as it has been the case in the past with the Al-Rashid Trust and Al Furqan.

332. The NPOs involved in TF (with or without their knowledge) can be international NPOs (i.e. outside of the regional control of the terrorist group) as well as NPOs founded in the areas under the control of terrorist organisations. The fundraising campaigns are conducted through social media, direct messaging, off- and online campaigns, and crowdfunding. Funds tend to flow through banks, other financial institutions, and unlicensed MVTS. In the end, funds are often converted to cash and logistical assets and services. One jurisdiction specifically mentions NPOs as being used to raise and move funds, that are then used to establish front companies, from which funds are managed.

333. Although individual terrorists, including FTFs, or small cells tend to fund themselves, they might use front NPOs as well. These NPOs are properly registered to solicit donations from unwitting donors, whose funds are then transferred in areas adjacent to conflict zones to NPOs with known affiliation to terrorist groups. This pattern of downstream diversion has been observed in several jurisdictions in connection with the financing of FTFs. Donations take place through direct bank transfer, online payment service providers, cash, and VAs.

334. Finally, in the context of EoRMT financing, the use of NPOs can involve fraudulent campaigns from operators falsely claiming to be a local operational arm of overseas charities or NPOs, but not having a legal presence in the country.

335. The typologies of the methods used to raise, move, and manage funds through the abuse of NPOs have remained relatively consistent since 2017, with the worth mentioning exception of the use of P2P payments, and crowdfunding and other online payments platforms.

© FATF-OECD 2025

Case studies: Abuse of NPOs for TF purposes

Germany

In 2021, Germany dismantled the fraudulent NPO Ansaar International e.V., along with eight associated sub-organisations, which financially supported terrorist groups such as Jabhat al-Nusra, Hamas[332], and Al-Shabaab[333]. These NPOs used a network of associations and individuals to solicit donations for humanitarian purposes, but the funds often did not reach their intended targets. Instead, they were routed through multiple intermediaries to obscure their origin and destination. Notably, FIU Germany benefited from information provided by Luxembourg regarding money pools. Funds were primarily raised through social media donation appeals and online shops, with transfers disguised under the guise of supporting humanitarian projects.

The funds were then passed to local "governors", converted to cash, or transferred to two designated Turkish accounts, and ultimately delivered via money mules. Due to their profiles being flagged by FIs, the primary actors were unable to open accounts and resorted to using straw men and establishing additional entities.

Criminal proceedings are ongoing before the Federal Public Prosecutor General, and in 2023, Ansaar International e.V. lost its appeal against the ban in the Federal Administrative Court.

Source: FIU Germany (See: Germany's Federal Ministry of Interior press release for more information ***www.bmi.bund.de***)
Note: The case references to domestic designated terrorist organisations Germany have no national designated sanctions list. The ban on associations and organisations is based on administrative and association law. The ban can be traced here: ***www.bmi.bund.de***; ***www.bverwg.de***; and ***www.verfassungsschutz.de***)

[332] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[333] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

Serbia

In 2019, Serbia convicted a group of seven individuals for terrorism-related offenses, including four for TF. The group established a sham NPO that publicly promoted tolerance and cooperation with authorities but secretly facilitated ISIL recruitment and provided logistical support for fighters traveling to Syria. The sham NPO was registered legally in Serbia, but its activities masked propaganda efforts and fundraising for ISIL operatives.

Funds were raised through donations, membership fees, and sales of publications, with the proceeds used to support fighters' travels to Syria. Some suspects used funds sent by family members abroad, including social benefits, to finance their journeys. The funds were transported via informal channels, such as personal couriers or occasionally through commercial banks.

Two convicts raised EUR 1,900 to purchase supplies for travel to Syria, while others contributed money or secured vehicles for the operation. One individual unknowingly facilitated the transfer of funds through his bank account, which were later used to support terrorist activities.

Source: Administration for the Prevention of Money Laundering, Serbia. See: *www.balkaninsight.com*

11. In-kind based methods

11.1. Trade-based terrorist financing

336. Trade-based terrorist financing (TBTF) is a value-moving method based on transferring in-kind goods and on dishonest billing. TBTF is defined as disguising the movement of value through the use of trade transactions in an attempt to finance terrorism, whether from legitimate or illegitimate sources[335]. Funds located abroad and aiming at financing terrorism are used to buy goods, which are then transferred where the beneficiary organisation operates. The latter will sell the goods, often in cash for greater opacity, and use the amounts earned to fund its activities. Such schemes allow for transnational transfers of value with lower risk of detection and provide beneficiaries with a justification on how revenues were generated. In practice, TBTF schemes can and do rely on the common TBML techniques and can also feature legitimate firms and transactions right through supply chain, until the funds are eventually diverted to terrorist organisations[336].

337. The key techniques being used to exploit trade-related activities for TF purposes can be different according to the stage of the export/import activity being conducted and/or the stage of the supply chain.

338. In addition to the core aspects of trade-based schemes, several methods can be implemented to further either disguise the origin and destination of funds or circumvent

[334] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[335] FATF and Egmont Group joint report on Trade-Based Money Laundering. Trends and Developments (2020)

[336] Ibid.

© FATF-OECD 2025

TF-related sanctions regimes. These include acquiring goods through less traceable means of payment, issuing fraudulent invoices—such as over-invoicing, under-invoicing, or multiple invoicing—misclassifying goods by declaring incorrect nomenclature or values in trade documents, conducting superficial transfers across multiple jurisdictions prior to final delivery, and executing nominal transactions between several shell companies.

339. Such methods can be used by structured organisations with international presence. Trade-based schemes can be facilitated when an organisation is not designated at multilateral level, as it opens possibility for rebounds before reaching the final destination of goods. Trade-based schemes can also involve import and export companies, freight forwarders, and custom brokers.

340. Examples underpinning this report include trade in commodities, precious stones, and international automobile transactions, notably involving stolen vehicles. In this context, authorities have identified instances where organised crime has leveraged proceeds from auto theft to finance various illicit activities, including terrorism. Canadian authorities reported that a significant portion of outbound financial flows to Hezbollah[337] has been frequently associated with the automobile trade. In particular, Hezbollah has reportedly used extortion to coerce individuals in Canada into fraudulently purchasing luxury vehicles and shipping them to Lebanon via the port of Montreal.

341. Such trade-based TF schemes can be countered through enhanced scrutiny of trade routes and stronger controls on import/export documentation.

11.2. Other in-kind methods

342. Besides trade-based schemes, in-kind goods can in rarer cases be used by terrorist individuals to store funds and transfer value.

343. In-kind storing and/or generating of value by terrorist networks mostly takes place through real estate. Switzerland observed that funds linked to TF, after being moved internationally, could then potentially be invested in Swiss real estate. Real estate investment is also reported by ESAAMLG delegations regarding regional and national groups such as ADF[338], the ISIL groups operating in Central Africa, and Al-Shabaab[339]. In addition to investing in real estate, Eastern African authorities have also noted a growing interest by terrorist groups, particularly ADF, in investment opportunities involving trading in livestock.

344. In 2021, the FATF reported that EoRMT groups have increasingly invested funds in the purchase of real estate. Often these properties are in structurally weak areas in which EoRMT actors often appear as the only interested parties. This real estate property then becomes a central hub for the group, giving it a convenient and secure venue for internal

[337] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001).

[338] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

[339] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). Al-Shabaab is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 751 (1992) concerning Somalia, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

meetings. EoRMT groups also use real estate property to increase their operational capacity and spread its ideas. For example, they are used for concerts, parties, martial arts events and training courses (physical and survival training).

345. Storage of gold or jewellery is also reported on rarer occasions. According to India, ISIL or Al-Qaida inspired individuals can use this storing method for small funds, either keeping assets themselves or having relatives hiding it. Madagascar also reports on gold storage in safe-deposit box, as well as gold being displaced on small quantities to remain under legal threshold and not to attract attention. Therefore, TF risks should be considered in the framework of AML-CFT regulation of the real estate sector, of precious metals and stones' trading, and of dealership of high value goods such as jewellery and watches. Furthermore, storage of high value goods can take place through rental of safe deposits.

346. In-kind donations toward terrorist organisations can also be observed. Since 2019, Zambia has noticed an increase of in-kind donations towards ADF[340], coupled with an upsurge in the receipt of food, shelter, and medical supplies. South Africa also reports cases involving ethnically or racially motivated groups where individuals offer their services or make their property available to support activities of the terrorist organisation. Nicaragua indicates that domestic terrorist groups receive not only cash donations but also logistical and material support, including food and clothing.

[340] Organisation designated under a supranational or national designation regimes established for the purposes of asset-freezing pursuant to UNSCR 1373 (2001). ADF is also subject to sanctions imposed by the UNSC Committee pursuant to resolution 1533 (2004) concerning DRC, and is monitored by the UN 1267 Monitoring Team due to its connections with ISIL, AQ or their affiliates, as reported by Member States.

© FATF-OECD 2025

Section 3: Terrorist Financing Risks Evolution and Anticipated Trends

347. TF methods are characterised by a relative continuity in the use of financing channels and schemes which have been documented for years; the acceleration of methods based on new technologies; and a growing interlinkage between financing methods of different natures. Evolutions of TF risks observed over the last years under the effect of combinations of materiality, institutional, demographical, technological, and ideological factors, are likely to continue in the coming years. It is therefore crucial to take into consideration those contextual factors and upcoming trends to anticipate and stand ready to face tomorrow's TF risks.

348. Nevertheless, these anticipated trends should be regarded as merely indicative, as they build on the information available at the time of drafting this report. New and unforeseen trends may emerge at any time, which is why jurisdictions are encouraged to continuously reassess the TF risks to which they may be exposed.

Geographical trends

349. ISIL-K continues to pose a significant threat in Afghanistan but also in Europe and Central Asia, where it actively seeks to recruit, and is regarded as posing predominant extra-regional terrorist threat[341]. The ISIL-K threat was augmented by a robust online propaganda apparatus and facilitated by remote logistical networks using the Russian language common to Central Asian States and North Caucasus regions of the Russian Federation, alongside with targeted propaganda in Pashtu, Turkish, Uzbek and other languages used in the region. Recent arrests evidenced the presence in Europe of numerous sympathizers from the Central Asian and North Caucasus diaspora with legal resident status who facilitated the relocation of ISIL-K operatives in the Schengen area and provided financial and logistical support to conduct opportunistic actions[342].

350. The volatile situation in the Syrian Arab Republic has been highlighted, noting the risk that stockpiles of weapons could fall into the hands of terrorists, as well as the concern about an estimated or approximately 42,500 individuals (by end of 2024), some with alleged links to ISIL, who remain in detention camps in the north-east. Various terrorist groups, mainly of contingents of FTFs, are still present and active in Syria. As noted by the UN 1267 Monitoring Team in its most recent report, in total, 40 individuals, groups, and entities listed by the UNSC as part of ISIL and AQ sanctions regime were linked in their designation with HTS[343]. The report also emphasised risks of ISIL regrouping in areas with reduced counter-terrorism pressure, specially along the Iraqi border, with Syria potentially becoming a renewed hub for FTFs' recruitment[344]. Finally, it also mentioned

[341] See the latest reports of the United Nations, e.g., Twentieth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, S/2025/72, January 2025; Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 ((2004) and 2253 (2015), S/2025/71/Rev.1, February 2025; UNSC Briefing on the threat posed by ISIL (Da'esh) to international peace and security, 10 February 2025; UNSC Meeting on strengthening African leadership and implementation of counter-terrorism initiatives, 21 January 2025.

[342] Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 ((2004) and 2253 (2015), S/2025/71/Rev.1, February 2025, paragraph 76.

[343] S/2025/71/Rev.1, paragraph 53 and following

[344] S/2025/71/Rev.1, paragraph 57

© FATF-OECD 2025

ISIL sleeper cells in Iraq capable of, inter alia, maintaining media platforms and fundraising via organised crime[345].

351. Beyond the potential impact of developments in Syria on terrorist threats, significant financial flows are also likely to arise in connection with refugee movements, reconstruction efforts, recovery initiatives, and humanitarian assistance. Jurisdictions' ability to monitor these flows—and to implement effective preventive measures against TF—will largely depend on the extent to which regulated financial services, particularly those involving institutional actors, are re-established within Syria. If informal financial activities remain predominant, the international community's ability to safeguard financial security will remain constrained. At the time of publication, the situation in Syria continues to be marked by significant uncertainty.

352. Critically, recent debates at the UNSC highlighted that sub-Saharan regions in Africa, and more specifically the Sahel, has emerged as the epicentre of global terrorism[346]. This shift has elevated the continent as a key priority for the UN Security Council in its efforts to counter terrorist threats, due to Africa's increasing role as both a target and a source of terrorist activities. These developments carry significant regional implications[347] and could have far-reaching consequences beyond the continent itself.

353. The UNSC recognises that Africa is home to some of the world's most active and dangerous terrorist groups, which operate across borders and tap into vast informal economies. As also noted throughout this report, these groups have been able to raise, move and store significant funds and resources through, inter alia, abuse of legitimate commercial enterprises, exploitation of natural resources, and proceeds from criminal activities including KFR, extortion and illicit taxation, the illicit trade and trafficking in cultural property, persons, drugs, and SALWs, further destabilising already fragile States[348]. Noting the financial connectivity among ISIL and Al-Qaida affiliates, the UN 1267 Monitoring Team highlights the importance of revenue generated by affiliates in Africa which are considered less susceptible to disruption, in part because they rely on informal channels and illicit sources[349]. For many terrorist groups operating in Africa, territorial control is crucial to their survival and expansion. UNSC's concern is also driven by the transnational nature of TF in Africa, as the cross-border nature of these activities further complicates efforts to disrupt the flow of funds. Terrorist organisations operating on the continent are expected to retain established financing methods, while increasingly

[345] S/2025/71/Rev.1, paragraph 66

[346] See *e.g.* also, Statement of Amina J. Mohammed, Deputy Secretary-General of the United Nations at the 9842nd meeting of the Security Council, 21 January 2025 and meeting coverage (SC/15971)—available at https://press.un.org. See also the Global Terrorism Index 2024, page 4, Institute for Economics and Peace—available at https://www.economicsandpeace.org

[347] United Nations, Security Council, 9633rd meeting, Maintenance of International Peace and Security, S/PV.9633, 23 May 2024

[348] United Nations, Security Council, Presidential Statement on Security Council Meeting, Open debate on African-led and development-focused counterterrorism: strengthening African leadership and implementation of counter-terrorism initiatives under the Security Council agenda item "Maintenance of international peace and security", 24 January 2025, See also Arria-Formula Meeting on Countering Terrorism in West Africa and the Sahel, 19 June 2024, New York

[349] Analytical Support and Sanctions Monitoring Team, thirty-fourth report submitted pursuant to resolution 2610 (2021) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2024/556), paragraph 98. Available at www.un.org

© FATF-OECD 2025

leveraging new technologies and adapting them to local contexts marked by conflict and political instability—particularly in regions such as the Horn of Africa.[350].

Decentralisation of terrorist financing operations

354. The continuing decentralisation of terrorist groups and their operations throughout the world is linked to a corresponding decentralisation in their financing methods, including the enhanced role of regional financial hubs and a potential further increase in self-financed cells, each adapting to the context-specific needs and circumstances of their operational areas. The diversification of funding sources and methods at a local level may further complicate efforts to disrupt larger financial networks.

355. Decentralisation may also result in transnational terrorist organisations intensifying strategies based on inspiring attacks by homegrown terrorist individuals and small cells based in foreign jurisdictions. In terms of TF risks, this could translate in continuous microfinancing strategies by lone actors and small cells' members. These strategies may involve the use of legitimately generated funds, proceeds from low-level criminal activity, and the transfer of small amounts through diverse channels—with an increasingly significant role played by methods leveraging digital innovations.

356. In a different dimension, decentralised financing through fundraising activities in the virtual world, could enable terrorist organisations to develop their own online ecosystems, potentially creating their own Metaverses with unique currencies for value transfer purposes or mere marketing[351].

Intensifying terrorist propaganda and fundraising

357. As noted above under Section 1, terrorist propaganda output remains extensive, in multiple languages, often trying to exploit events in the Middle East to appeal to new recruits and attract additional resources[352], including donation campaigns through VAs.

358. In several regions, propaganda is framed around the defence of marginalised and vulnerable populations, often invoking alleged abuses by security forces and auxiliary actors to legitimise its narratives[353]. Some sources note a certain degree of convergence between different ideologies that inspired recent terrorist attacks, especially in relation to lone actors[354]. This is also linked to an expansion of online propaganda and calls for violence exploiting the unfolding situation in the Middle East, and other political tensions and conflicts.

359. There is an increasing risk of online radicalisation and recruitment targeting young people and minors exploited by terrorist groups through the use of alternative Internet platforms and encrypted chat applications. Most terrorist groups continue to operate

[350] [Placeholder for CTED's Gaps Assessment on Africa CFT]. This was also highlighted during the January 2025 FATF JEM discussions.

[351] Project CRAAFT, "Virtual Threats: Terrorist Financing via Online Gaming", Gonzalo Siaz, 2025, available at https://static1.squarespace.com citing to Council of the European Union, 'The Metaverse in the Context of the Fight Against Terrorism', Special Report, 2 June 2022.

[352] Thirty-fifth report of the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 ((2004) and 2253 (2015), S/2025/71/Rev.1, February 2025, paragraph 1, 9, 61, 72, 74, 79; S/2025/72, paragraph 4

[353] Ibid., paragraph 13

[354] E.g., Europol European Union Terrorism Situation and Trend Report (2024)

© FATF-OECD 2025

active crowdfunding campaigns via dedicated propaganda channels, including magazines and encrypted messaging channels.

360. Some groups, like ISIL-K, are implementing a regionalisation and internationalisation strategy that has increasingly focused on extending its reach into Central Asia, as well as appealing to associated diaspora elements elsewhere, especially in parts of Europe and in Russia[355]. More recently, ISIL-K has established a Russian-language media branch that is rapidly expanding its online reach. This development reflects growing integration between its Russian propaganda operations and its Tajik and Uzbek components, particularly on Telegram, indicating enhanced coordination and an increased strategic focus on media production. Despite effective governmental efforts to disrupt terrorist communications and propaganda networks, researchers note that terrorist groups are highly likely to continue exploiting Telegram to advance their agendas, including propaganda dissemination, recruitment, and fundraising activities[356]. Threat actors are also migrating to other, lower-profile channels to continue operations.

Evolving demographical trends

361. Several delegations report on increasingly young radicalised and terrorist individuals, to the point that according to the Global Terrorism Index 2025[357], one in five persons arrested for terrorism in Europe is legally a minor[358]. In terms of CFT measures, this trend may come with additional challenges as those young individuals are in many cases likely to rely on someone else's financial resources and to show even more proficiency in using opportunities offer by digital innovations. Of particular concern is the increasing use of video games as a means to influence children and young people towards engagement in terrorist-related activities[359].

362. Against the backdrop of the already visible trend regarding the lower age of radicalised individuals, the use of AI by terrorist groups might pose a particular risk in the recruitment and radicalisation of young people, including through more targeted and tailored propaganda[360].

363. As noted earlier in this report, gendered roles in TF, as well as impact of CFT measures on certain gender groups, also require continued analysis and monitoring.

Combined use of various TF methods with modern technologies

364. Although cash and HOSSPs remain the prevalent methods used to move money for terrorist purposes, accounting for most TF-related transfers, there is also an increase of their use in combination with digital technologies and payment methods[361]. The growing convergence of methods used to raise and move funds—for example, combining online

[355] Perspectives: ISKP intensifying online propaganda targeting Russia and Central Asia | Eurasianet, Lucas Webber and Louise Meloy, September 2024.
[356] Perspectives: ISKP intensifying online propaganda targeting Russia and Central Asia | Eurasianet, Lucas Webber and Louise Meloy, September 2024.
[357] Institute for Economic & Peace (IEP), Global Terrorism Index 2025.
[358] Op. Cit.
[359] See also, S/2025/71/Rev.1, paragraph 72.
[360] Ibid., paragraph 9
[361] UNSC Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes," S/2025/22, January 2025

© FATF-OECD 2025

fundraising in virtual assets with the subsequent use of HOSSPs or cash couriers—amplifies the challenges associated with each individual technique. This blended approach merges the difficulties of detecting physical cross-border cash movements with the complexities of tracing sophisticated virtual transactions[362]. As discussed earlier, the emerging use of digital HOSSPs is expected to raise new challenges for CFT enforcement.

365. Globally, the expansion in terrorist use of digital platforms is a growing concern. The use of digital methods in the form of electronic wallets, sale of prepaid mobile cards, and VAs is expected to continue and become even more pervasive and significant. Connected to the increasing use of VAs and progressive successes in tracing VA transactions, is the growing exploitation of obfuscation techniques (e.g., shared digital wallets, mixers, chain-hopping) as well as a shift towards the use of alternative VAs which are promoted as more private and secure [363]. It remains to be seen whether the upswing in prices of VAs will make any significant impact on the on their use by terrorists, including for purposes of investment.

366. In addition to the trends analysed with respect to online gaming in Section 2, researchers caution about the gaming industry as constantly evolving with the development and introduction of new technologies. The emergence of blockchain technologies, the growing presence of VAs, and new platforms where these items would converge (such as the 'Metaverse') might alter the threat landscape[364].

367. In the banking sector, it is likely that exclusively online services will continue to attract an increasing number of clients. Whether this trend will have an impact on TF risks will depend on how robust applicable AML/CFT regulations in jurisdictions are and how effectively they are implemented by online banking service providers. As of 2025, vulnerabilities partly originate from the fact that many online banking actors are relatively recent and thus lacking maturity in terms of due diligence. It therefore remains to be seen whether their compliance procedures improve with time. Vulnerabilities linked to remote business relations may prevail in some extent, even though identity checking solutions may improve and spread more broadly. Conversely, online banking actors could take advantage of the fact their data are already fully digitalised and structured to set-up efficient automatic screening processes.

368. Still in the banking sector, the use of virtual IBANs is expected to become increasingly widespread, as they address legitimate needs such as accounting consolidation and the prevention of discrimination. However, virtual IBANs can also contribute to obscuring the final destination of funds and concealing their beneficial owners. The potential misuse of virtual IBANs for TF should therefore be monitored in the coming years; and traceability issues related to virtual IBANs should continue being addressed in multilateral discussions regarding payment transparency.

369. Another trend to observe carefully within regulated financial sectors, including VASPs, is the sophistication of document forgery with the use of digital innovation, including AI. The use of fake or stolen credentials and identification documents has already been observed across a broad spectrum of sectors vulnerable to TF misuse, such as opening bank accounts, accessing MVTS, and engaging with VASPs. Authorities should therefore work closely with the private sector to develop solutions to verify identity,

[362] Ibid.

[363] *Cut the Cord,* D2.1 Report on Terrorist Financing Threats and Trends, January 2022, available at CTC-D2.1-Report-on-Terrorist-financing-threats-and-trends.pdf

[364] Project CRAAFT, "Virtual Threats: Terrorist Financing via Online Gaming", Gonzalo Siaz, 2025, available at https://static1.squarespace.com

© FATF-OECD 2025

including through digital onboarding, taking into account emerging risks linked to AI and other innovations. Overall, delegations should remain vigilant to the risks of AI misuse to evade due diligence processes.

370. As explained above, the increase in the abuse of technologies for TF purposes goes along with the uptake in their use in society overall.

Rise in politically motivated and EoRMT-type of attacks

371. Concerns have been raised about the possibility of a spike in politically motivated violence, given the levels of political polarisation and instability that have been seen over the past five years[365]. In addition, as noted in the 2025 Global Terrorism Index, there has been a sharp increase in antisemitic violence and hate crimes across different parts of the world, with attacks on synagogues recorded in Europe, Australia, and the US[366]. As described in Section 1, tracing financial trails related to this type of terrorist attacks comes with its own set of challenges, including inconsistent designations and proscriptions, as well as low scale and visibility of financial activity in the preparation of attacks.

Convergence with criminal activities

372. The convergence between TF and organised crime networks is likely to continue. Terrorist organisations of different types have been reported as generating significant revenues through illicit economic activities and criminal methods; and vulnerabilities allowing for such financing schemes are unlikely to be fully addressed in the short-run as it would require significant capacity-building investment and major operational improvement by authorities. A trend in continuing linkages between EoRMT groups and criminal networks has also been noted[367].

373. In many regions where criminal groups rely primarily on cash, such convergence may mean that cash will remain the prevalent method for TF-related transactions.

374. One aspect to monitor closely is the risk of terrorist organisations increasingly reaching out to professional money launderers to hire their services. Such trend could result in ever more complex TF schemes, involving international transfers undermining traceability of financial flows, legal persons obstructing beneficial owners' identification and diversification of financing channels.

375. The scale of TF through online crimes and frauds, that could range from relatively simple scams to larger ransomware attacks, can also be expected to grow in parallel with the general increase in these illegal activities[368].

Challenges in maintaining humanitarian action

376. Impartial humanitarian action, including the provision of medical supplies, shelter and food, is essential in many parts of the world for the enjoyment of essential social and

[365] Global-Terrorism-Index-2025.pdf , page 36
[366] Global-Terrorism-Index-2025.pdf , page 36
[367] Europol European Union Terrorism Situation and Trend Report (2024)
[368] *Cut the Cord,* D2.1 Report on Terrorist Financing Threats and Trends, January 2022— available at CTC-D2.1-Report-on-Terrorist-financing-threats-and-trends.pdf

© FATF-OECD 2025

economic rights, including the rights to food, safe drinking water, and adequate access to health care[369].

377. Armed conflict contexts in which terrorist groups and/or FTFs operate create increased risks for humanitarian aid diversion for TF purposes, as reported by several jurisdictions. This also raises challenges for impartial humanitarian action where measures to counter TF may result in negative unintended consequences on the provision of vital humanitarian aid[370].

378. Humanitarian action follows four core principles: independence, neutrality, unconditionality and impartiality. As a result, humanitarian action cannot be targeted, and there cannot be any screening of its beneficiaries[371].

Growing risks of resource shortage

379. Food insecurity, whether related to conflicts or natural disasters, has become critical in some regions and can lead to increasing food raids and excessive looting by terrorist groups[372]. As mentioned earlier in this report and documented by UN sources, water shortages or pollution can play conflict intensifier and may be used as a tool by terrorist groups to delegitimise government institutions or obtain financial gains from controlling and/or taxing access. Some EoRMT organisations have used climate change-related rhetoric's, including climate-driven migration, to support their narratives.

380. Overall, even though research on the issue of climate change and the evolution of terrorist threat remains in its infancy, it suggests that the increasing frequency of extreme weather events and increased competition for resources are likely to create greater opportunities for exploitation by terrorist groups in the future[373].

[369] [Placeholder for reference to UN Global Compact Guidance on Ensuring respect for human rights while taking measures to counter the financing of terrorism]

[370] UN CTED, Trends Tracker on Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014 – 2024, 12 November 2024, page 14—available at https://www.un.org/securitycouncil/ctc. For more information see FATF High-level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards on undue targeting of NPOs (2021); UN CTED's study on The interrelationship between counter-terrorism frameworks and international humanitarian law, January 2022—available at, https://www.un.org/securitycouncil/ctc; ICRC: Politics and principles: The impact of counterterrorism measures and sanctions on principled humanitarian action https://international-review.icrc.org

[371] United Nations General Assembly resolution 46/182

[372] See, e.g., S/2025/71/Rev.1, paragraph 35.

[373] *E.g., Institute for Economics and Peace (IEP),* Global Terrorism Index 2023, featuring David Wells, Global Security Consultant "Climate Change, Terrorism and Potential Implications for P/CVE"—available at https://www.economicsandpeace.org.

© FATF-OECD 2025

Section 4: Recommendations

Addressing the transnational dimension of TF risks

381. TF remains a global phenomenon. The majority of inputs received from the FATF Global Network delegations deal with terrorist organisations operating transnationally. Many of the fundraising methods described in this report are inherently transnational, including the smuggling of various goods, online donation campaigns, diversion of humanitarian aid, and diaspora extortion. Funds directed towards terrorist organisations also cross borders through multiple channels, such as the physical transport of cash, informal value transfer systems, VAs, and formal financial services. FTF-related funds also follow their movements across jurisdictions. Terrorist organisations are furthermore reported taking advantage of regulatory weaknesses of some jurisdictions, when setting financing schemes based on financial services, the abuse of legal entities, or trade-based practices. When enabled through modern technologies, TF-related transfers can be conducted across borders instantly.

382. Such global dimension of TF risks thus calls for multilateral responses. Effective cooperation in TF investigations and prosecution, based on coherent criminalisation of the offence and robust information sharing channels compliant with international law, is also essential to dismantle terrorist networks operating in multiple jurisdictions.

383. Full and coherent implementation of FATF Standards will contribute to upgrading and harmonising legal frameworks globally, reducing opportunities for terrorist organisations to benefit from regulatory discrepancies and loopholes.

384. Multilateral designations of terrorist organisations, notably under the UNSC sanction regimes, still appear as the most overreaching sanction instrument to obstruct TF, especially in relation to tackling transnational TF schemes. For this reason, designations under UNSC framework should remain a priority and proactivity by delegations is encouraged in that regard[374]. Operationalising national mechanisms for freezing of terrorist funds and assets pursuant to resolution 1373 (2001), including a designating mechanism with adequate due process consideration, as well as a dedicated mechanism to address foreign asset-freezing requests, is also key in preventing terrorists from accessing funds across jurisdictions.

Addressing regional and local specificities

385. Besides the global dimension of TF, the updated TF risk analysis also highlights regional specificities that must guide our collective action. TF risks vary depending on materiality factors such as territorial control by terrorist organisations, proximity with armed conflict, porous borders, and the type of terrorist groups and individuals present in a region.

386. One trend observed by FATF delegations is the growing role regional and local affiliates play in the financing of larger terrorist organisations. This is especially salient

[374] Given the existing risk that designated individuals and entities use sanctions evasion techniques to undermine screening controls and avoid the implementation of the asset freeze, the Monitoring Team recommends that the Committee encourage Member States to provide detailed financial information on the updated standard form for listing, especially regarding the identification of the final beneficiary, the use of cryptocurrencies in financial transactions and the connections with high-risk jurisdictions (S/2025/71/Rev.1, paragraph 132).

© FATF-OECD 2025

regarding sub-Saharan Africa, which occupies a significant share of the report as many delegations consider it is confronted to some of the world's higher TF risks. Sub-Saharan delegations furthermore insist on the fact that some local branches of terrorist organisations can generate profit locally, without relying on international donations or support from core-organisations. Their fundraising strategies often consist of criminal activities such as extorting local populations, illegal exploiting natural resources, KFR, and smuggling of drugs, weapons or humans. In other regions, branches of larger organisations, are also seen as increasingly active and autonomous in their financing, notably the ISIL-K.

387. Another trend reported by several delegations is the growing endogenous threat posed by lone actors in certain jurisdictions. Such isolated individuals, displaying increasingly young age, are likely to radicalise online, and plan attacks with low-cost modus operandi. They can therefore rely on microfinancing strategies, based on licit sources of revenue (salaries, social benefit, family support) or illicit ones (small scale fraud, retail drug trafficking, theft).

388. Such diversity of risk exposure among regions and jurisdictions means the present comprehensive TF risks analysis could usefully be complemented by more detailed national and/or supranational risk analyses. It also highlights the relevance of designation regimes established at regional or national levels, pursuant to UNSCR 1373, to address region or country-specific terrorism risks. Domestic regimes of asset freezing appear as particularly relevant when dealing with endogenous threat from lone actors: their transactions can be difficult to detect as suspicious since they mainly consist of low value operations, so asset freezing regime targeting individuals instead of single transactions are a useful complementary instrument.

Addressing TF risks through effective implementation of FATF Standards

389. The present analysis also identifies a diversity of channels and schemes used by terrorist organisations and individuals to raise, move and store funds, as well as a growing interlinkage between various methods.

390. Methods based on informal channels and practices, such as transportation and use of cash, unregistered remittances, and HOSSPs are still very predominant. They are still attractive for terrorist organisations and individuals for the anonymity and opacity they afford, as well as their ability to facilitate the transfer of value beyond the reach of regulated sectors. Those channels are also available in conflict and remote areas, where financial services are underdeveloped. Even though their exposure to TF risks has been documented for years, these methods continue to evolve, including under the effect of technological innovation: online services, mobile applications, and other digital solutions are quickly developing and becoming more common in TF schemes.

391. The report highlights that room for improvement remains in several sectors covered by the FATF Standards. Progress has certainly been made at the global level, as indicated by the fact that most delegations consider that terrorist organisations and individuals increasingly avoid traditional financial services, often subject to relatively more mature regulation. However, MVTS, which are AML-CFT obliged entities under FATF Standards, are still perceived as significantly exposed to TF risks. The fact that mitigation has remained insufficient from the FATF report on Emerging TF Risks in 2015[375] to the present analysis calls for new workstream to be launched at the FATF level to assess

[375] FATF Emerging Terrorist Financing Risks (2015)

© FATF-OECD 2025

remaining vulnerabilities and ways forward to better implement preventive standards toward MVTS providers.

392. VAs and VASPs are also widely considered by delegations as seriously exposed to TF risks. They are indeed vulnerable because they offer opportunities for anonymous transactions, for instantaneous international transfers, and because regulatory frameworks remain underdeveloped in many jurisdictions. Advancing toward effective implementation of FATF Standards with regards to VAs and VASPs across all jurisdictions is thus critical to efficiently mitigate TF risks and avoid the emergence of "crypto havens". This should especially take place through the roadmap to strengthen implementation of the FATF Standards on VAs and VASPs adopted in February 2023 and monitored by the FATF Virtual Asset Contact Group. In its targeted update on implementation of standards on VAs and VASPs, FATF insists in particular on the urgency for all jurisdictions to rapidly comply with the Travel Rule, with obligations to licensing, registering and supervising VASPs, and to address risks related to unhosted wallets.

393. At the same time, terrorist groups are perceived to use VA in combination with other financing channels, including cash. Therefore, expansion of VA usage for terrorist purpose may partly depend on the development of conversion to fiat money infrastructure, including in conflict and high-risk areas. Nevertheless, despite its serious exposure to TF risks, blockchain technology can also provide investigative opportunities to LEAs. For this purpose, ensuring authorities can rely on available and effective blockchain analysis tools is pivotal, which calls for continuous dialogue among delegations and such service providers.

394. TF risks posed by physical cross-border transportation of cash are still considered high in most parts of the world, as terrorists continue taking advantage of porous borders to move fundings, to smuggle persons, arms, and other illicit goods. This even appears as one of the main TF concerns by several jurisdictions, including in sub-Saharan Africa, where custom management remains a prominent challenge. Mitigating these risks requires strengthened border control capabilities, supported by technical assistance programmes and the exchange of good practices, particularly in relation to mandatory declaration frameworks and controls.

395. Several delegations also reported on terrorist organisations conducting financing activities through legal persons, whether it is by generating revenue from an actual business activity, or by using front or shell companies to dissimulate TF-related operations. Should convergence between TF and organised crime—and especially with regards to money laundering—keep strengthening, TF schemes could get increasingly sophisticated, potentially involving legal persons more often. Effective implementation of the FATF Standards on legal persons, including norms on beneficial ownership transparency, is thus all the more critical to CFT.

Addressing TF risks in sectors which are not covered by the FATF Standards

396. The present analysis also identifies issues related to sectors that are not covered by FATF standards. In this regard, and with respect to UNSC resolution 2462 (2019), all States are urged to assess specifically their TF risk and to identify economic sectors most vulnerable to TF, including but not limited to non-financial services, such as, inter alia, the construction, commodities and pharmaceutical sectors[376], States are also encouraged to

[376] UNSC resolution 2462 (2019), paragraph 14

© FATF-OECD 2025

assess and address potential risks associated with new financial instruments, including but not limited to crowd-funding platforms, that may be abused for the purpose of TF[377].

397. The report highlights both vulnerabilities and documented instances of abuse across a range of sectors that fall outside the scope of AML/CFT measures. These include industries such as mining, as well as digital platforms offering diverse services—from messaging and gaming to other forms of online entertainment. The use (involuntary or due to negligence and low risk awareness) of many formal and informal sectors to facilitate TF activity, be it to sell trafficked goods, launder money or call for donations, makes it extremely challenging to tailor effective responses.

398. This is also the case of social media, certain types of crowdfunding platforms and messaging applications, as detailed in Section 2. Social media can be exposed to additional risks when they provide in-house payment services or monetisation features, as those can offer opportunity for terrorists to proceed transactions without any obliged entity conducting due diligence. This exposure calls for greater outreach towards social media and messaging applications actors[378] to ensure their proper level of awareness on TF risks and enforcement of mitigation measures, including self-regulation and content moderation specific to TF. Overall, jurisdictions are encouraged to carry out evidence-based assessments of TF risks associated with social media, including identification of specific features used for integration with payment services[379]. PPPs are a pivotal instrument to help to ensure that the CFT efforts of social media companies are informed and effective. Overall and as noted below, PPPs have also served as a useful forum for the authorities to disseminate regular guidance to the private sector, including risk indicators.

399. Synergies with projects tackling more broadly links between tech actors and terrorism, such as the Christchurch Call, the Tech for Good initiative or Tech Against Terrorism, could also be further explored.

Addressing the impact on humanitarian activity

400. The report has noted several challenges related to addressing TF risks in the context of delivery of humanitarian aid and the work of charities. In this regard, the UNSC has urged States, when designing and applying CFT measures, to take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law[380]. Yet, according to the joint Report prepared by UN CTED and the Analytical Support and Sanctions Monitoring Team issued in 2020, 45% of States lacked an institutional framework to consider the effects of CFT measures on humanitarian activities[381]. In 2022, UN CTED further reiterated that only a

[377] UNSC resolution 2462 (2019), paragraph 20(d)

[378] See also, United Nations Security Council Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes" (S/2025/22), January 2025, paragraphs 20(i) and 22(f)—available at S/2025/22

[379] United Nations Security Council Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes" (S/2025/22), January 2025, paragraphs 18(f)—available at S/2025/22 citing to Asia/Pacific Group on Money Laundering and Middle East and North Africa Financial Action Task Force, Social Media & Terrorism Financing Report(2019).

[380] UNSCR 2462 (2019), paragraph 24.

[381] S/2020/493, paragraph 83

© FATF-OECD 2025

handful of States have adopted dedicated measures to evaluate, and eventually mitigate, the impact of CFT measures on exclusively humanitarian activities, including in conflict zones with active terrorist activity[382].

401. In December 2024, through the unanimous adoption of resolution 2761 (2024), the UNSC decided to maintain the exemption of humanitarian aid providers from asset freeze measures imposed by the ISIL and Al-Qaida sanctions regime. The exemption provided clarity that the provision, processing or payment of funds, other financial assets, or economic resources, or the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance or to support other activities that support basic human needs by the UN and other stakeholders defined in paragraph 1 of resolution 2664 (2022), are permitted and are not a violation of the asset freezes imposed by the UNSC or its Sanctions Committees.

Addressing TF risk through broader technical assistance cooperation

402. TF risks are also to be understood in relation with broader capacity building challenges. To finance their activities, terrorist organisations can take advantage of weak State capacities: inability to assert authority in certain remote areas, insufficient border control, weak government services, lack of infrastructures, corruption, and so on. In these contexts, terrorist organisations can find themselves in situations to derive meaningful profit from large-scale illegal activities: taxation-like extorsion, exploitation of natural resources, drug trafficking, or KFR. Fighting such practices does not circumscribe to TF issues but should take place in the framework of broader security and law enforcing policies. Therefore, efforts to tackle TF risks related to territorial control by terrorist organisations and to profit-generating criminal activities, also benefit from technical assistance and capacity-building cooperation projects pursuing broader objectives. It is therefore important for the FATF community to make sure that broader cooperation projects integrate CFT challenges and build on FATF Standards to promote robust and effective frameworks. To do so, it should be further explored how FATF could mobilise its internal expertise and could facilitate the mobilisation of its Global Network's expertise, to contribute to technical assistance program were adding a CFT dimension would be relevant.

403. Addressing technologically advanced TF methods also requires advanced expertise and capacity. In this regard, the UNSC Counter-Terrorism Committee specifically recommends developing and enhancing, in an ongoing manner, the capacity of relevant national authorities to follow the money more effectively, including through parallel financial investigations in terrorism cases, with the use of new analytical methods, tools and technologies, as well as the requisite independent oversight and review mechanisms[383].

[382] UN CTED, Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions , December 2022, page 22..

[383] United Nations Security Council Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes" (S/2025/22), January 2025, paragraphs 22(c) and 22(m)—available at S/2025/22

© FATF-OECD 2025

Multi-stakeholder approach to understanding and addressing TF risks, including through public-private partnerships and raising awareness to the private sector

404. Maintaining a continuous understanding of the risk's jurisdictions are exposed to, by conducting regular risk analysis exercises, are also at the core of the FATF Recommendation 1. In doing so, jurisdictions are encouraged to utilise a multi-stakeholder approach, including effective interaction and exchanges between the relevant national authorities, the private sector, civil society and academia, to develop a comprehensive picture of the existing and evolving TF risks informed by a diversity of experiences and perspectives and better understanding both the benefits of these technologies and the scale of the threat and impact on different categories of sectors and populations, including local communities, as well as region-specific realities, thus enabling the development of a tailored and proportionate response.

405. The UNSC Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism has also recommended conducting regular, inclusive, and evidence-based TF NRAs that take into account each State's unique operating climate and context as well as global and regional TF trends[384].

406. It has further been explicitly recommended to develop robust PPPs to share information, enhance understanding of evolving trends, increase the knowledge and skills of relevant experts and stakeholders, including gatekeepers, and help to strengthen the integrity of the financial sector[385]. Such partnerships should include dialogue between financial intelligence units and the relevant FinTech sector with regard to data-sharing as part of suspicious activity reporting, with a clear legal basis for the sharing of information, including criteria and purposes for which information may be shared and the entities with which it can be shared.

407. In response to requests expressed by the private sector through the TPC, and in addition to the development of risk indicators[386], the FATF should consider additional actions to enhance its support to the private sector. FATF could also consider developing targeted communication strategies, such as newsletters. FATF could as well mobilise its expertise and network to provide awareness-raising and training activities to private sector staff, including through in-person and online training initiatives.

Follow-up to this comprehensive TF risks analysis

408. Finally, it is worth underlining that the present report aims at offering an as comprehensive as possible overview of worldwide TF risk as of 2025, and that it builds on knowledge shared by the FATF Global Network members, relevant literature, and other

---

[384] United Nations Security Council Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes" (S/2025/22), January 2025, paragraphs 18(a) and 18(e)—available at S/2025/22

[385] UNSCR 2462 (2019); United Nations Security Council Counter-Terrorism Committee, "Non-binding guiding principles on preventing, detecting and disrupting the use of new and emerging financial technologies for terrorist purposes" (S/2025/22), January 2025, paragraph 22 (l)—available at S/2025/22; UN CTED, Analytical Brief on 'Establishing effective public-private partnerships on countering the financing of terrorism, December 2023—available at https://www.un.org/securitycouncil/ctc

[386] See Annex A.1

© FATF-OECD 2025

publicly available information. Still, risk analysis must remain an ongoing process, as new TF schemes can emerge or be detected. Therefore, our collective understanding of TF risks will have to be continuously updated and enriched in the coming years, through national and supranational risk analysis, sectoral risk analysis, or emerging risks assessments.

409. This comprehensive update has set the foundation for the FATF to take stock of its CFT measures, and to launch new initiatives to strengthen its efforts, in line with the continued prioritisation of this objective.

© FATF-OECD 2025

Annex A. Terrorist Financing Risk Indicators on Evolving Methods and Techniques

410. The indicators provided below have been derived from a sampling of the data provided by delegations as part of their responses to the project's questionnaires[387] and consultation of previous FATF published reports. They should not be considered as a comprehensive list.

411. The TF Risk Indicators on Evolving Methods and Techniques reflect the additional inputs provided to the well-established and documented general financial indicators that can also be indicative of other financial crimes, including money laundering (ML). Many of these indicators are broad in nature, and do not in themselves constitute suspicious activity. It is important to bear in mind that in many cases a single indicator cannot warrant suspicion of TF or provide a clear indication of such activity. However, it could prompt further monitoring and examination, as appropriate.

412. Consultation of previous FATF published reports is encouraged, such as Crowdfunding for Terrorist Financing[388]; Illicit Financial Flows from Cyber-Enabled Fraud[389], Virtual Assets Red Flag Indicators of ML/TF[390]; ML/TF Risks arising from Migrant Smuggling[391]; Trade-Based ML Risks Indicators (where applicable)[392]; Detecting Terrorist Financing Relevant Risk Indicators[393]; Ethnically or Racially Motivated Terrorism Financing[394] and detecting EoRMTF Risk Indicators[395]; Risk of Terrorist Abuse in Non-Profit Organisations[396]; and The role of Hawala and Other Similar Service Providers in ML/TF[397].

Indicators relevant to customer behaviour

413. Knowledge of a customer plays a vital role in understanding the nature of operations conducted. Useful indicators relevant to identifying changes in the customer behaviour towards TF purposes are as follows:

a) Recognisable radicalisation or change of character through a change in lifestyle, online presence and/ or behaviour.

---

387 [By 11 October 2024] Call for inputs- Comprehensive Update on Terrorist Financing Risks and [Call for inputs by COB 24 March] Comprehensive Update on TF Risks: Second Questionnaire.

388 FATF Crowdfunding Terrorism Financing (2023)

389 FATF Egmont Group and Interpol joint report on Illicit financial flows cyber-enabled fraud (2023)

390 FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020)

391 FATF Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling (2022)

392 FATF and Egmont Group joint report on Trade-Based Money Laundering Risk Indicators (2021)

393 FATF confidential reports available for delegations (2016 and 2021 versions).

394 FATF Ethnically or Racially Motivated Terrorism Financing (2021)

395 FATF confidential report available for delegations (2021)

396 FATF Risk of Terrorist Abuse in Non-Profit Organisations (2014)

397 FATF The Role of Hawala and Other Similar Service Providers in ML/TF (2013)

© FATF-OECD 2025

b) Customers who is inquisitive about transaction thresholds and how an institution processes transaction to and from a high-risk jurisdiction.

c) Records of travel or intention to travel to high-risk jurisdictions or online discussions around travelling to these jurisdictions.

d) Anonymous clients or sanctioned individuals or entities are involved.

e) Customer has previously been investigated by law enforcement for terrorism related offences.

f) Customer has a history of penalties related to AML/CFT or a history of suspicious and unusual activity.

g) Identification issues and proxies:

h) Customer provides multiple variations on their name, address, phone number or additional identifiers.

i) Customer uses incorrect spelling or providing variations of their name when conducting funds transfers to high-risk jurisdictions.

j) Customer uses proxies for the establishment and or activity with an account.

k) Customers avoid personal contact or send intermediaries.

l) Customer becomes evasive or unwilling to provide necessary identification document.

m) Customers are reluctant to provide information or request to cancel the transaction as soon as important missing information is questioned.

n) Customer provides falsified documents when opening an account or conducting a once-off transaction.

o) Customer is the holder of a replacement identification card.

p) Recurrent use of the same address, phone number across multiple unrelated accounts.

q) Customers open account on behalf of entity potentially linked to terrorism.

r) Young individuals (between the ages of 17-26 years) open accounts and withdraw or transfer funds shortly afterwards.

s) An account in which several individuals hold signature authority, and the individuals do not have any family or business relationship.

t) An account opened by a person/entity that has the same addresses or contact numbers as of other persons/entities without any apparent economic or plausible reason.

u) Businesses operating with limited staff despite high transaction volumes.

v) Entities located or active in geographical areas that are known to finance or support terrorist activities or in which terrorist organisations operate, or in areas bordering or crossing such areas.

w) Customers information consists of encrypted email accounts.

x) Customers borrow from multiple banks without clear financial justification.

© FATF-OECD 2025

a) Customers suddenly adopt new financial instruments, allowing further concealing of the origin or destination of funds (P2P transfers, ATM withdrawals, third party payment processors, prepaid cards).

Indicators relevant to the economic profile of the customer

414. Ongoing monitoring of the economic profile and any change in this transaction history enhances risk identification. The general indicators relevant to this provided by delegations are as follows:

Relevant to transactions

a) Disposing of meaningful personal assets or belongings in an unusual manner, particularly with urgency or without regard for personal financial gain.

b) Structured transactions to avoid reporting thresholds.

c) Transactions involving multiple customers remitting funds to the same beneficiary or multiple beneficiaries in high-risk jurisdictions.

d) Customer remitting funds to multiple beneficiaries in a higher-risk jurisdiction.

e) Large number of wire transfers made by a person in small amounts in an apparent effort to avoid identification requirement.

f) Transactions to or from entities or individuals in multiple countries without an apparent purpose.

g) Individual, located in a high-risk jurisdiction or a neighbouring country, receives international transfers from multiple unrelated individuals in a short period of time.

h) Multiple low-value domestic transfers to a single account and cash deposits made by multiple third parties.

i) Transactions may lack clear purpose or involve intermediaries to obscure the origin.

j) Transfers involving business accounts inconsistent with declared business activities or transaction volumes.

k) Structured cash deposits and withdrawals, especially if the customer is known to be unemployed and if deposits emerge in complementarity with regular pay checks.

l) Transfer of funds between business accounts and personal accounts of business officeholders that is inconsistent with the type of account held and/or the expected transaction volume for the business.

m) Remittance of funds to a new identity preceded by the cancellation of a previous remittance to a different beneficiary.

n) Unexpected reactivation of payment instruments or accounts that had remained inactive for a long time, which, also based on the person's profile, suggests that he/she has been abroad for a long time for unjustified reasons.

o) Suspicious or unverified purposes for sending funds, such as “family support” or “help for a person”.

© FATF-OECD 2025

p) Use of anonymity-enhancing electronic money or VAs, particularly when converted into legal tender.

q) Use of prepaid cards in a suspicious manner, such as loading funds and immediately withdrawing large amounts or one person holding numerous cards.

r) Conducting a large initial deposit when entering a business relationship while the amount funded is not consistent with the customer profile.

s) Immediate withdrawals that lack explanation or inconsistent transactions patterns are present.

t) Taking out consumer credit, followed by cash withdrawals of a significant portion of the loaned funds and/or transfers abroad.

u) Total or almost total withdrawal of assets from accounts or life insurance policies.

v) Frequent foreign currency cash deposit which are below threshold, followed by immediate withdrawal in foreign jurisdiction.

w) Opening of a safe deposit box on behalf of a commercial entity when the business activity of the customer is unknown, or such activity does not appear to justify the use of a safe deposit box.

x) Multiple cash deposits into personal account described as "donations" or "contributions to humanitarian aid" or similar terms.

y) Transactions with entities linked to terrorism activities.

Relevant to spending activities

a) Sudden or inconsistent changes in spending behaviour or lifestyle exceeding declared income.

b) Customers make cash payments with unclear sources.

c) Payments are made for the acquisition of special knowledge or qualifications, such as pilot's licenses, weapons permit or driving licenses for large vehicles/ships.

d) Purchases of items with both civilian and military applications, also referred to as dual-use goods, (e.g., camping, survival, and medical equipment)

e) Purchases of chemicals, minerals, precious metals, firearms, firearm making kits, ammunition, explosives, and/or tactical gear.

f) Payments to online retailers, charities, individuals or businesses that are known, or believed to sell violent extremist paraphernalia, literature, and/or merchandise.

g) Payments to subscriptions or social media causes that are known, or believed to promote violent extremist paraphernalia, literature and/or merchandise.

h) Monthly and/or one-time payments are made to extremist media outlets and/or propaganda websites.

i) Acquisition of a property intended for use by an unincorporated or incorporated association with links to an extremist organisation.

j) Individual/ entity facilitating and/or selling merchandise, tickets, and/or donations that may be linked to violent extremist groups.

© FATF-OECD 2025

k) Financial transactions aimed at training or recruiting individuals for violent or illegal activities.

l) Transactions linked to ideologically-motivated violent extremism, including purchases of extremist propaganda or frequenting known extremist platforms.

m) Flights, accommodation, visas, car rentals to or within high-risk jurisdictions.

n) Flights, accommodation, visas, car rentals to high-risk jurisdictions on behalf of third parties.

Indicators relevant to geographic risks

415. For the purposes of this section, "High-risk or Higher-risk Jurisdictions" refer to: jurisdictions identified where there are indications that individuals or organisations in that jurisdiction are at a heightened risk of being involved in TF; and/or there are active terrorist or TF threats due to current or recent conflicts in the jurisdiction; and/or or there are indications that the jurisdictions' population are targeted to support terrorist activities domestically or abroad. Identified risk indicators relevant to geographic risk include any financial activity that involves or is associated with a high-risk jurisdiction. This could include:

Customer financial activity in high-risk jurisdictions

a) Customer or associates being located or associated with a high-risk jurisdiction.

b) Customer making online payments for services or ATM use in high-risk jurisdictions or close to areas with active terrorism threats, or in areas bordering conflict zones.

c) Frequent travel to high-risk jurisdictions.

d) Sending or receiving international transfers to and from high-risk locations.

e) Conducting business in the proximities of areas with active terrorism.

f) Opening or owning a bank account in a high-risk jurisdiction.

g) Customer's IP addresses are not consistent with the expected location data of the entity.

h) Retailers in a high-risk jurisdiction receiving regular, round amount transfers via MVTS from overseas remitters, especially where the value or regularity of the payments is inconsistent with expectations for that retailer's line of business.

i) Transactions involving foreign currency exchanges are within a short time followed by funds transfers to higher risk locations.

j) Frequent use of credit cards to withdrawals funds from various locations rather than the usual customer's area of residence especially in areas neighbouring conflict zones.

k) Use of online payment platforms from regions neighbouring or deemed to be a transit location to conflict zones.

l) Fundraising through natural person accounts linked to high-risk jurisdictions.

m) Preference for remittance services to send funds near terrorism-active zones

© FATF-OECD 2025

Travel related operations

a) Flights, accommodation, visas, car rentals to or within high-risk jurisdictions.

b) Flights, accommodation, visas, car rentals to high-risk jurisdictions on behalf of third parties.

c) Sale or disposal of personal items prior to travel, including family homes.

d) Individuals attempting a cross-border transport of physical money to conflict zones or other localities with significant deficiencies in their AML/CFT systems.

Indicators relevant to product or services among sectors subject to AML/CFT regulations

416. Due to the gamut of products and services available, these indicators cannot easily be ordered in a sequential manner and often overlap with other indicators such as geographical risk. Also, as already stated, the presence of one such an indicator does not automatically indicate TF, and further examination may be required. Indicators put forward by delegations include:

a) An account in which several individuals hold signature authority, and the individuals do not apparently have any family/business relationship.

b) An account opened by a person/entity that has the same addresses or contact numbers as of other persons/entities without any apparent economic or plausible reason.

c) A person/entity maintaining an account apparently associated with a terrorist organisation or having similar ideology as of a terrorist organisation.

d) Wire transfers by an individual or entity to/from the high-risk jurisdictions or to countries of specific concern including but not limited to countries designated by national authorities and/or countries included in FATF's list of high-risk jurisdictions.

e) Person/entity receiving or sending funds through wire transfers to the parties, which are not related to its line of business.

f) Transactions conducted or accounts maintained by the persons/entities proscribed by the authorities of foreign jurisdictions and international organisations, including persons/entities associated with them.

g) Newly opened banking account is being operated on the instructions of third party for cash deposits.

h) Use of products which abet anonymity (e.g., bearer negotiable instruments, anonymity-enhanced virtual assets, VA mixers etc.).

i) Frequent use of credit cards to withdraw funds from various locations rather than the usual customer's area of residence especially in areas neighbouring conflict zones.

j) Use of online payment platforms from regions neighbouring or deemed to be a transit location to conflict zones.

Indicators relevant to trade and commercial entities

417. Observable trade and commercial entities of heightened concerned for TF included companies involved in the following sectors: precious metals and minerals, natural

© FATF-OECD 2025

resources, shipping import and export and chemical research or manufacture. The types of products and services that may be involved in TF through these entities ranged from payment transfers from the importer to the exporter to more sophisticated financial products, such as letters of credit, documentary collections, and guarantees. TF can also rely on trade-based money laundering schemes, using international trade to conduct illicit transactions and disguise origins of funds. Risk indicators for these methods include:

a) Individuals associated with violent extremist activity conducting trade transactions

b) Trade involving items originating from crisis areas or conflict zones.

c) High-risk commodities (precious metals and minerals, energy commodities).

d) Import of goods where the payment for the goods is made by a third party.

e) Unusual financial activity by an entity exporting goods to conflict areas or high-risk regions for TF.

f) Indications that traded items are stolen or looted.

g) Inconsistent trade practices, complex intermediaries, and use of unusual or high-risk shipping routes.

h) Vague descriptions, inconsistent pricing, and missing or counterfeit trade documents.

i) Company address appears to be inconsistent with the business in which it is engaged.

j) Company lacks online presence or has an online presence inconsistent with its purported business activities.

k) Company name that mimics more-established competitors.

l) Company's number of staff inconsistent with its trading volume Recently established company making high-volume or high-value trades Reluctance or refusal to provide information on a product's destination Unfamiliarity with an imported or exported product's intended use

m) Issuing multiple invoices for same shipment with different descriptions of goods, their value, or number of items shipped

n) Customs documents falsified, missing, rejected, or duplicative of old documents

o) Contracts supporting complex or regular trade transactions appearing unusually simple. (e.g., copying a "sample contract" structure available online)

Indicators relevant to the abuse of NPOs

418. As FATF clearly indicates in its standards, not all NPOs are exposed to significant TF risks, and some may represent little to no risk at all. However, many FATF delegations have reported cases of NPOs being abused by terrorist organisations and individuals for financing purpose. Such schemes can consist of legitimate NPOs being involuntarily forces into TF operations, being created for the purpose of disguising funds, access to materials and equipment and or to exploit their networks.

© FATF-OECD 2025

419. To fight such practices while at the same time allowing legitimate NPOs to continue conducting their activities, the risk-based approach promoted by FATF Standards is all the more important. The purpose behind these list of risk indicators is not to disrupt the legitimate activities NPOs and/or humanitarian aid channels conduct, but to help competent authorities and reporting entities detect and disrupt the abuses of NPOs for the purposes of TF.

General indicators

a) NPO operates in high-risk jurisdiction.

b) The use of funds is not consistent with purpose for which it was established.

c) The amount of funds at the disposal of the NPO is not consistent with its profile.

d) NPOs operating in conflict areas have wired significant funds to local companies whose activities are not related in any way to humanitarian services.

e) Crowdfunding and social media used to solicit donations, then online presence vanishes or shuts down.

f) The NPO has been incorporated recently.

g) Lack of documentation regarding internal procedures of the NPO.

h) Unclear designation and objectives of the NPO.

i) Use of multiple personal and business accounts or the accounts of NPOs to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

j) NPO authorises a third party to use the account to send funds abroad, especially to high-risk countries.

Relevant to NPO activities

a) NPOs making cash transactions without adequate justification.

b) An NPO has projects and/or partners in an area where terrorist entities are known to operate.

c) An NPO has unreported activities, or an NPO has programs, partners, or a financial report that do not tally with its activity report.

d) An NPO disburses funds to initiatives which are deemed vulnerable targets for terrorist groups or individuals.

e) Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organisation.

f) Untypical increase in the frequency and number of financial transactions on an NPO accounts or, conversely, an NPO holds funds in its account for a very long period of time.

g) Unusual or atypical large cash withdrawals (bearing in mind that NPOs can legitimately turn to cash when operating in certain jurisdiction with few financial services).

© FATF-OECD 2025

Relevant to NPO's executives and other staff

a) An account is opened in the name of an NPO with an agent who is not a member of the board of the NPO.

b) NPO or NPO representatives use falsified or conflicting documentation.

c) An NPO or its administrators are linked to third parties that support or are engaged in terrorist activity.

d) An NPO member transfers money out of the organisation's account to a personal account.

Indicators relevant to establishing links between terrorism-related activities and organised crime

420. It has been observed that collaboration between criminal and terrorist groups exists, including shared resources and joint operations. The interconnected nature of these two illicit activities demonstrates the fluidity across crime types, which often obfuscates a clear understanding of the predicate crime at play. However, observation of indicators specific to TF risks with the following indicators may hint at connections between TF and organised crime:

a) Frequent large cash transactions.

b) Use of complex corporate structures like shell companies.

c) Terminology relating to drug, weapons and/or human trafficking.

d) Entities associated with these activities when funds appear to be orientated towards exploitative activities.

Indicators relevant to new and emerging technologies

421. Crowdfunding and the use of VAs are the two main reported technologies used more frequently within the TF lifecycle. Many of the indicators relating to the customer and the economic profile of the customer as detailed above are also observed across these two streams.

Relevant to social media

a) Use of specific religious terminology and images or references to specific milestones (example "*Baghouz*" battle or "*Ghuwayran*" prison break).

b) Use of certain hashtags such as #camphol #camproj #Imprisoned sisters (with no reference to any terrorist group).

c) Online discussions about travelling to high-risk jurisdictions.

d) Inquiring on how to proceed to an anonymous online donation.

Indicators specific to crowdfunding platforms

a) Entities located in geographical areas that are known to finance or support terrorist activities or in which terrorist organisations operate, or in areas bordering or crossing such areas, are involved in the crowdfunding campaign.

© FATF-OECD 2025

b) Non-transparent or anonymous entities are involved in the crowdfunding campaign.

c) Lack of information about the purpose, goals, and ultimate beneficiaries of the crowdfunding campaigns; vague project descriptions.

d) Inconsistencies between donation calls and donor comments.

e) Discrepancies between the IP address associated with the customer's account and the IP address from which transactions are initiated.

Indicators specific to Virtual Assets

a) Use of crowdfunding, FinTech, or VAs linked to extremism or radicalisation.

b) Transfers to and from VA platforms with inconsistent or unexplained transaction patterns.

c) Use of P2P exchange websites, mixing or tumbling services, or anonymity-enhanced VAs.

d) Attempt(s) to trade the entire balance of VAs or withdraw the VAs and attempts to send the entire balance off the platform.

e) Multiple users sharing the same device to control their wallets within the same VASP.

f) VA's customer funds originate from or are sent to a platform that is not registered in the jurisdiction where the customer or the exchange is located.

g) Operations in which several clients of the same VASP have a similar counterparty registry, revealing that they act in a coordinated manner, especially in those cases in which there is a high transactional activity among them, and especially if there is a coincidence of IP or devices used among these accounts.

h) Funds that originate from or whose destination is an address identified as suspected of being related to terrorist activities or their financing (through public lists, open-source information, virtual asset intelligence companies, etc.), even when the exposure to such addresses is indirect.

i) Operation in which the customer acts as a virtual asset exchanger, with a personal account, consisting of receiving funds from external addresses that are exchanged on the spot for other currencies and remitted to the same external address (or to another that is linked in some way to the initial address).

j) The party carries out transactions with virtual assets involving several different types of virtual assets or multiple money accounts or uses cryptomats to perform several transactions of a lower value, when there is no economic justification for such a thing (i.e. regardless of higher fees for such transactions).

© FATF-OECD 2025