An overview of terror financing risk

Yehuda Shaffer

8.10.26

In this presentation

- Background
  - TF risk
  - Criminalization of TF
- TF detection Cycle
- Recent FATF/MONEYVAL MER TF results
- TF typology update
  - FATF TF update
  - TF typologies from EU TE-SAT 2026 · Europol Terrorism Situation and Trend Report
- Conclusions

Myths you have been told about TF

- No consensus on what terrorism is - political
- TF always involves small amounts of money
- Difficult to detect - like a needle in a haystack
- ML preventative measure are good enough for TF as well
- Screening for TFS is sufficient

Legal Framework

- Terror definition – "Any violent act against civilians…to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act"

  (Article 2 -International Convention for the Suppression of the Financing of Terrorism, 9 December 1999)

- A successful terror group, as any other criminal organization, is one that is able to build and maintain an effective financial infrastructure

  (FATF- guidance for financial institutions in detecting Terrorist Financing)

Obligation to Prevent Terror

"…are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature, and calls upon all States to prevent such acts and, if not prevented, to ensure that such acts are punished by penalties consistent with their grave nature;

United Nations S/RES/1566 (2004)
Security Council Distr.: General
October 2004 8

2022 FORBS - World's 10 Richest Terrorist Organizations

	Organization	Est. annual revenue	Main area	Main income source
1	Taliban	~$2.5bn	Afghanistan, Pakistan	Taxes and levies
2	Houthis (Ansar Allah)	~$2bn	Yemen	Taxes on companies
3	Hezbollah	~$1.2bn	Lebanon, Syria	Iranian aid
4	Al-Qaeda and affiliates	~$600m	Global	Taxes
5	Hamas	~$500m	Gaza, West Bank	Taxes and levies
6	PKK	~$250m	Türkiye, Iraq, Syria	Drug trafficking
7	ISIS and affiliates	~$150m	Global	Taxes and protection money
8	Real IRA	~$70m	UK, Ireland	Illicit tobacco
9	Kata'ib Hezbollah	~$50m	Iraq, Syria	Iranian aid
10	Palestinian Islamic Jihad	~$35m	Gaza, West Bank	Iranian aid

So where is all this money?

Terror organizations use laundering methods because of the need to:

- Disguise the source and purpose of their funds
- Disengage themselves from their financiers

IO9 and risk

- What is the primary Risk profile of a Jurisdiction?:
  - “Collecting Jurisdiction”(e.g. through NPO)
  - “Movement Jurisdiction” (Inflows outflows, monitoring wire transfers from HRJ (jurisdiction specific - not only FATF listed)
  - “Jurisdiction where TF funds are used”



FATF REPORT

Terrorist Financing Risk Assessment Guidance

July 2019



Box 2.6. Monaco (MONEYVAL): Assessing TF Risks for International Financial Centres with low domestic terrorism risk

In April 2018, Monaco held a two-day workshop along with eight other financial centres and TF experts to consider the specific TF risks facing financial centres and the information they could draw on in order to identify, assess and understand these risks. The participants identified ways in which financial centres may be misused for cross-border movement of terrorist funds, including flow-through of terrorism funds, service provision, use of complex structures, abuse of philanthropy, and use of funds generated domestically by illicit activities. Participants also discussed potential information sources to identify financial linkages between financial centres and high-risk countries for terrorism and TF, many of which are presented in this Guidance (refer to paragraph 40 above).

Bets practice to identify TF vulnerabilities in financial centres:

- the extent of financial linkages with jurisdictions with active terrorist organisations and/or conflict zones (e.g. data on fund inflows/outflows by jurisdiction, including when available: data on bank deposits, correspondent banking, investments, use of ATMs abroad to withdraw funds from accounts, incoming and outgoing wire transfers, and loads and spends in respect of prepaid cards);
- the extent of trade linkages with jurisdictions with active terrorist organisations and/or conflict zones, and intelligence and open source information on links between the trade centre and funds or assets (including cargo) linked to designated individuals or entities and their associates;
- the extent to which business relationships and one-off transactions are carried out with parties who are in or are linked to target jurisdictions (including whether financial institutions play an important role as service provider or correspondents for individual customers or FIs located in high risk jurisdictions for terrorism), and the features and characteristics of those relationships or transactions;

- the extent to which financial or administration services are provided from the financial or trade center in respect of the import or export of goods or other trading activity that could be used for terrorism or to finance terrorist activities;
- the extent to which the financial or trade center is used by foreign PEPs (in light of the possible link with state-sponsored terrorism);
- levels of awareness of TF and trade expertise among the private and public sectors, and ability to detect suspicious behaviour;
- anomalies in available data (e.g. differences in the reported volume of exports from jurisdiction A to jurisdiction B to the volume of reporting imports by jurisdiction B from jurisdiction A).

Several major ICIJ investigations have highlighted terror-related complex structures:

1. The Panama Papers (2016)

Offshore shell companies connected to **Hezbollah** and rogue states like **Iran** and **North Korea** used layers of anonymous shell companies across multiple jurisdictions, making it nearly impossible for law enforcement to track the true beneficial owners.

2. The FinCEN Files (2020)

The investigation detailed how global banks moved money for entities linked to **Al-Qaeda**, **the Taliban**, and **Hezbollah**, even after receiving warnings from U.S. authorities. Illicit actors relied on complex layers of correspondent banking networks, shell firms, and nested accounts to mask the origin and destination of terror funds.

3. The Ericsson List (2022)

The files exposed corporate bribery and illicit protection payments to **ISIS (Islamic State)** in Iraq to secure transport routes for telecom equipment. Funds were funnelled through complex supply-chain loops, slush funds, third-party contractors, and fake invoices to conceal corporate engagement with a terrorist organization.

Example - **Assad's cousin** - Rami Makhlouf, a cousin of Syria's dictator, Assad - OFAC blacklisted in 2008
The issue of reliance on 3rd parties

"If HSBC didn't have an issue with him, then I think we can also accept him."

Later Zollinger told Süddeutsche Zeitung: "In retrospect my comment in the e-mail was wrong, which I regret."

Properly assessing the terror financing risk in financial centers

- Looking at inflows and outflows
- Learning about 1373 designations in target jurisdictions (not only 1267)
- Checking the UBO domicile profile
- Risk based EDD
- The danger of reliance on other`s CDD
- Multi jurisdictional approach with regard to complex structures (whether legal persons or arrangements)
- Attention to State sponsored terror (Through PEPS in HRJ)

RECOMMENDATION 5	TERRORIST FINANCING OFFENCE

5.1 Countries should criminalise TF on the basis of the Terrorist Financing Convention[13].

5.2 TF offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).[14]

5.3 TF offences should extend to any funds whether from a legitimate or illegitimate source.

5.4 TF offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

5.5 It should be possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances.

5.6 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of TF.



FATF GUIDANCE

CRIMINALISING TERRORIST FINANCING

(Recommendation 5)

Principle of Guilt

32. Many countries apply a principle of guilt (also expressed as "schuldprinzip" or "nulla poena sine culpa") as a fundamental element of criminal law. This principle requires that there is a fault on the part of the offender in order for a criminal offence to be committed, and that any penalty is proportionate to this fault. In some legal systems, the application of the TF offence to the provision of funds or other assets to an individual terrorist for a purpose entirely unrelated to terrorism may come into conflict with this principle, because the act of providing funds or other assets would be criminalised on the basis of the identity of the person receiving them, and not on the basis of their intended or actual use. The principle may also be invoked because the person who provides funds or other assets did not know or could not foresee that any harm would result from their actions.

Principle of Guilt

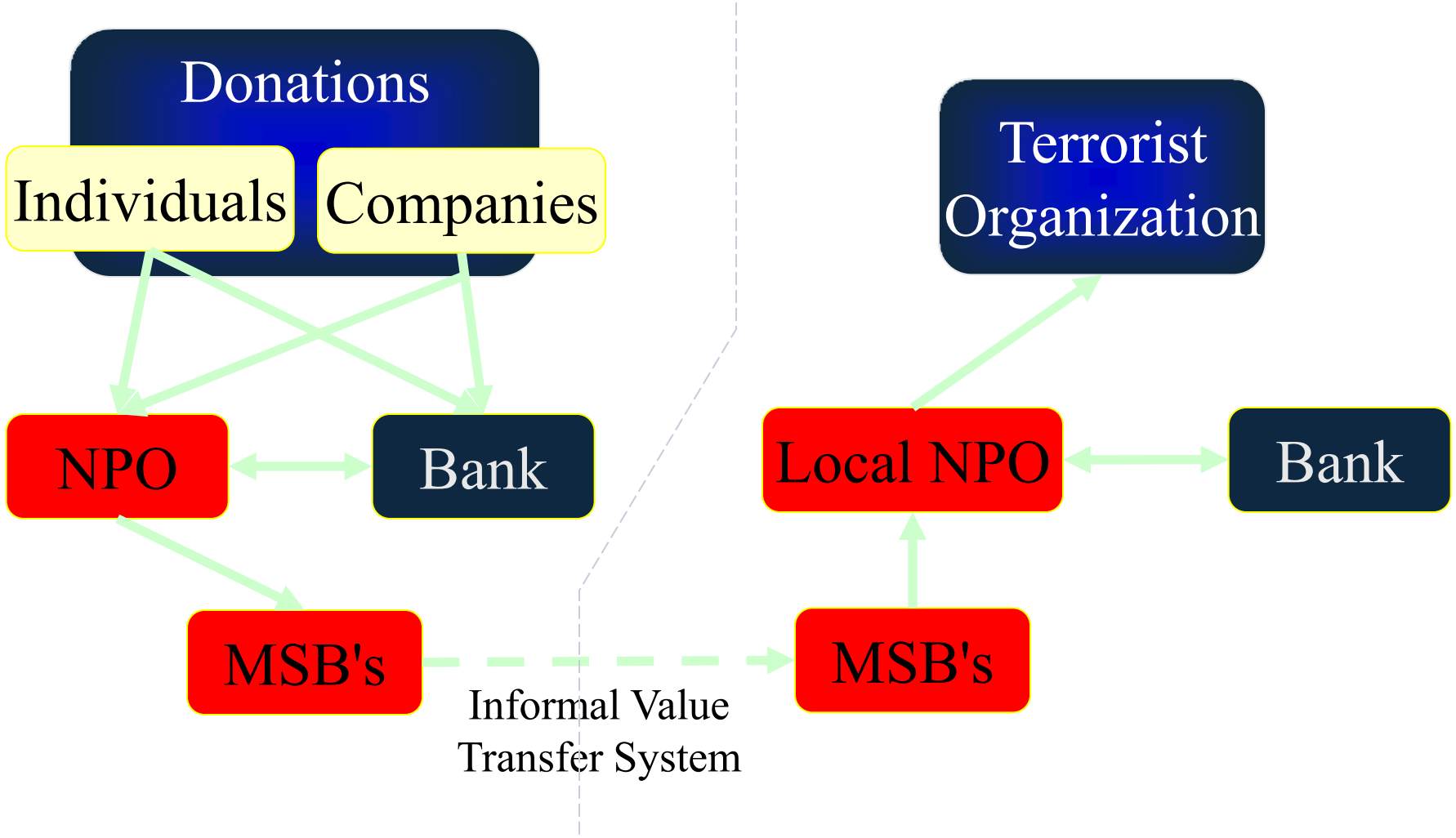
33. Whether there is a conflict between R.5 and the principle of guilt depends on how the requirements of R.5 are interpreted – specifically the requirement that "Countries should criminalise… the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts...", which is sometimes referred to as the requirement to criminalise the financing of terrorist organisations and individual terrorist for any purpose. There does not seem to be any conflict between the principle of guilt and the criminalisation of financing a terrorist organisation – since the purposes of a terrorist organisation can be assumed to be terrorist purposes.

2 examples

UK – Charities commission report on Interpal - Hammas

US - Holdern V US - on Material support to the PKK

Terrorism funding through NPOs
A typical “money trail”



COMPLIANCE

Inquiry Report

Palestinians Relief and Development Fund (Interpal)

Registered Charity Number 1040094



Interpal – The Charities commission report

- In 2007 raised more than 5 m £ of which at least 1.5 m £ were sent to Occupied Palestinian territories - and distributed by “local partners”
- The report examined several allegations against Interpal
- The commission noted that the inquiry had confirmed that the charity had maintained clear financial audit trails in their delivery of aid for humanitarian purposes. However:
- 1. The trusties had not taken sufficient rigorous steps to investigate allegations about some of their local partners.
- 2. Criticized the link of Interpal and the “Union of Good” and specifically of Dr. Mustafa
- 3. Due diligence and monitoring procedures were in place but not sufficient – recommended action to publish guidelines for local partners

Findings related to the trustees' actions

64. The Inquiry took into account the limitations on the trustees arising from the operational challenges of the Occupied Palestinian Territories. Nevertheless, the Inquiry found that the trustees had accepted the responses from the local partners without adequate further investigation.

65. Given the serious nature of the allegations, the Inquiry would have expected the trustees to have engaged actively with their partners in a manner consistent with the seriousness of the allegations being raised. The Inquiry noted that Funding Agreements were in place with the local partners[43] which set out how the Charity's funds could be used, and the conduct expected of the local partners. The Inquiry was told that the Charity sent questionnaires to four local partners asking them about the truth of the allegations made against the committees. However, the information provided in the four completed questionnaires received by the Charity from four local partners and shown to the Inquiry was, in the Inquiry's view, inadequate; for example in response to the question: *'Does your charity urge hatred and violence? Or do your employees do so?'* one zakat committee replied: *'The society goals don't encourage incitement on hatred or violence. Employees of the society don't practice any activity in this regard.'* A different zakat committee replied to the same question with: *'We don't support hatred or violence, and none of our staff use this method. Our goal is to help Palestinian women and children.'*

40 See paragraph 47.

41 See Issue 4 below.

42 See footnote 27.

HOLDER, ATTORNEY GENERAL, et al. v . HUMANITARIAN LAW PROJECT et al

SUPREME COURT OF THE UNITED STATES

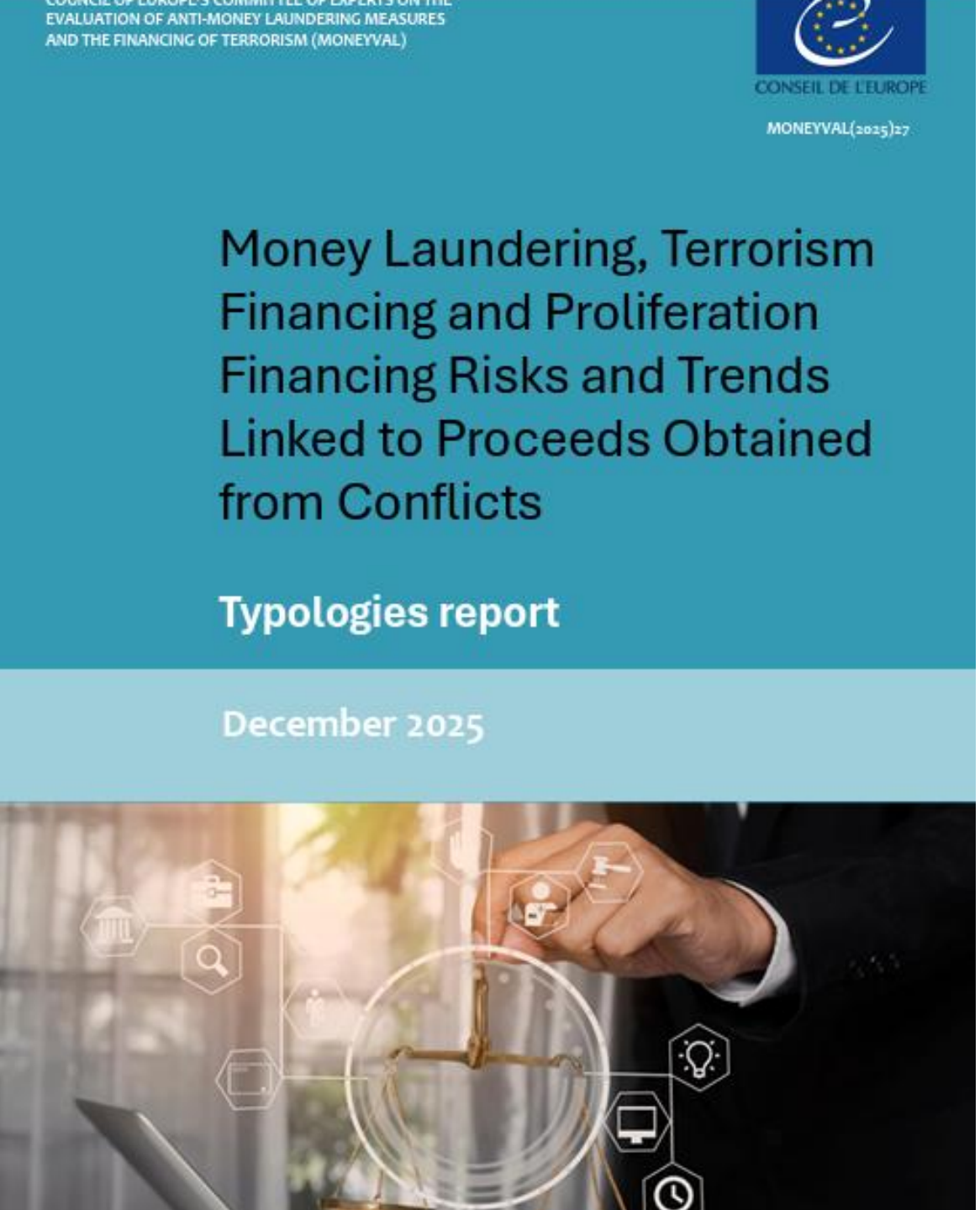
.

certiorari to the united states court of appeals for the ninth circuit

No. 08–1498. Argued February 23, 2010—Decided June 21, 2010 *

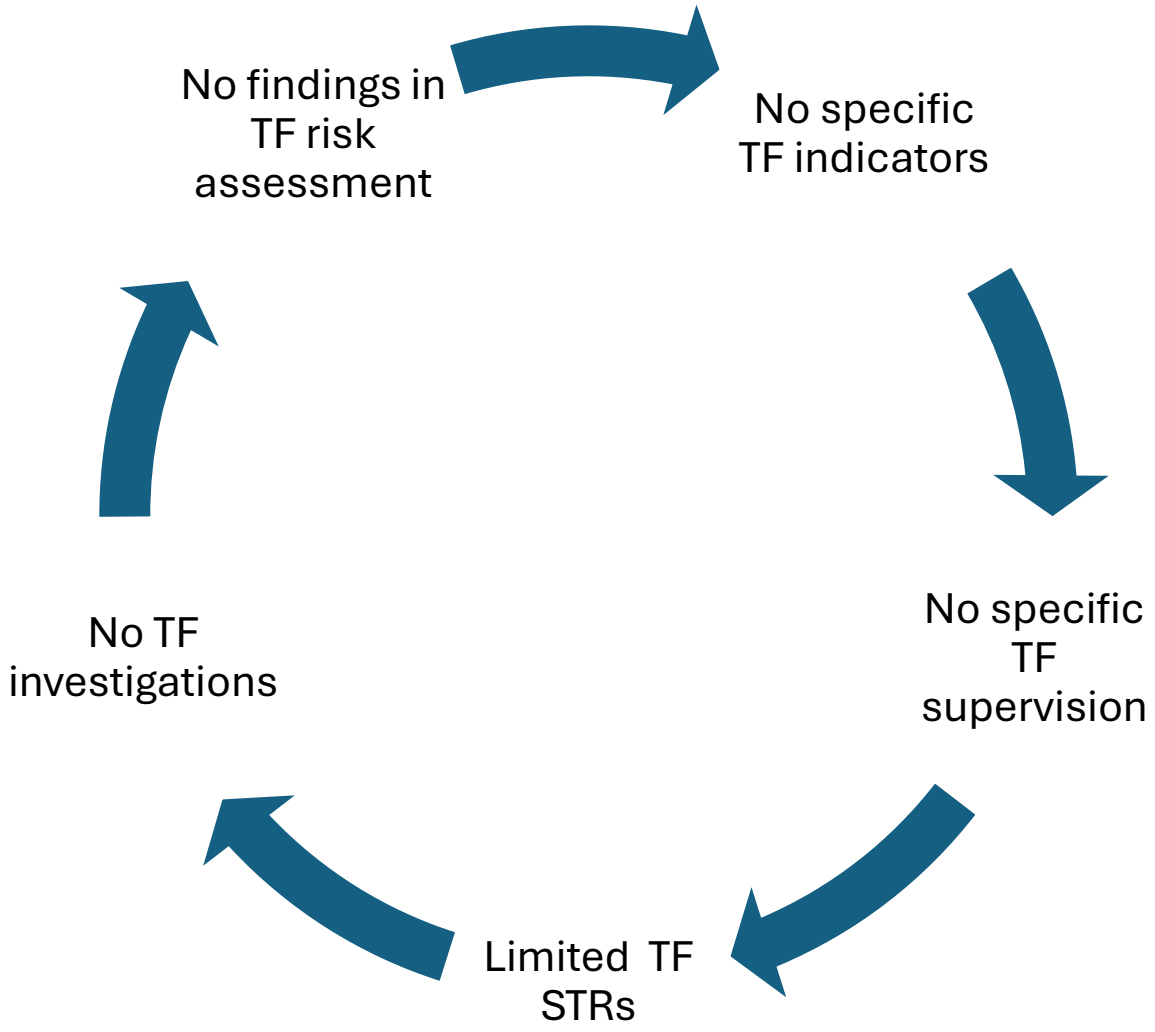
HOLDER, ATTORNEY GENERAL, et al. v .
HUMANITARIAN LAW PROJECT et al

"…it is wholly foreseeable that directly training the PKK on how to use international law to resolve disputes would provide that group with information and techniques that it could use as part of a broader strategy to promote terrorism, and to threaten, manipulate, and disrupt. Teaching the PKK to petition international bodies for relief also could help the PKK obtain funding it would redirect to its violent activities. "

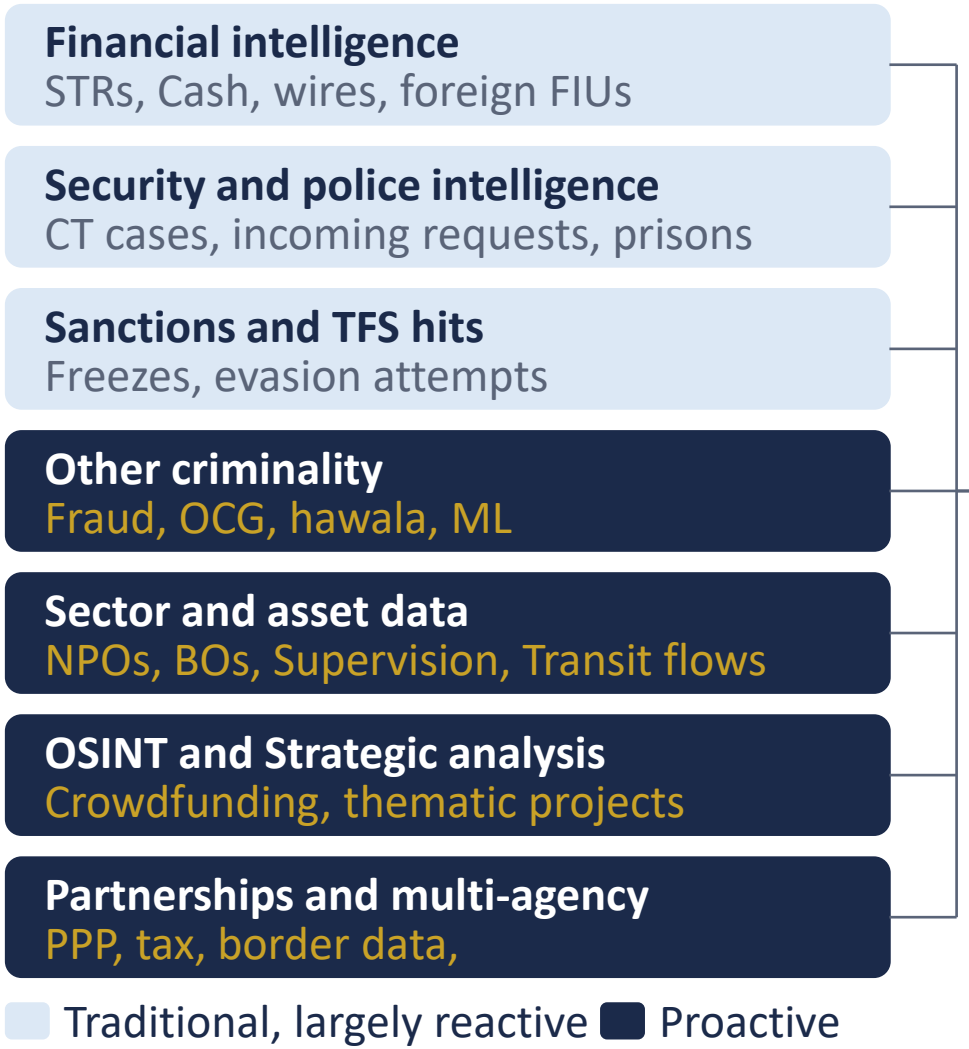


Conflict-related risks remain insufficiently reflected in national risk assessments (NRAs):

How can we break the invisible TF detection cycle ?



Where should TF cases come from?



9.1 How well and in what circumstances is TF activity identified and investigated? To what extent do the investigations identify the specific role played by the terrorist financier?

TF identification and investigation

9.2 To what extent is TF activity (including different types of TF cases) prosecuted and offenders convicted?

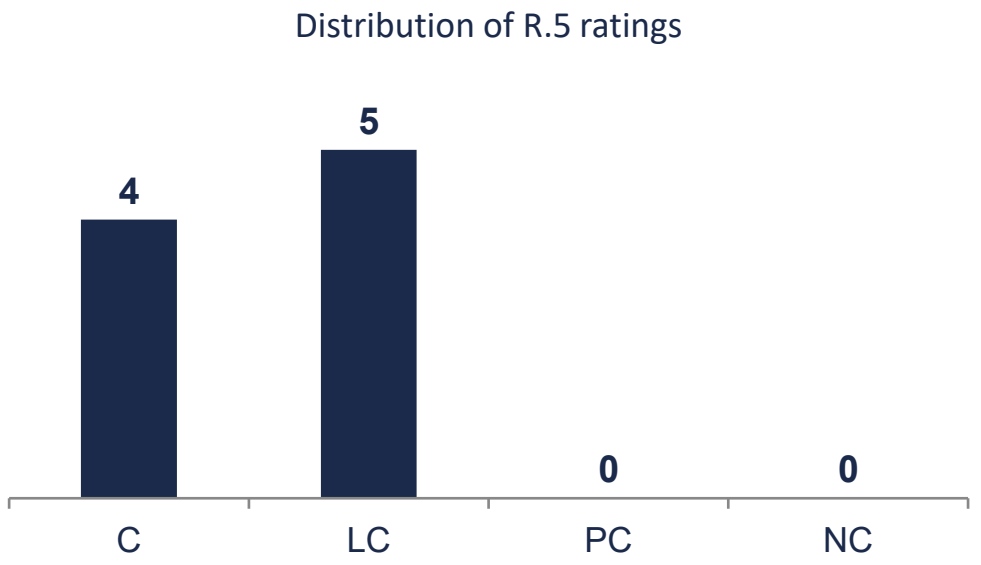
Comparative analysis) of the first 9 MERs under the FATF 2022 Methodology

- R.5 (technical compliance) and
- IO.9 (effectiveness

Belgium · Malaysia · Italy · Austria · Singapore
Latvia · Serbia · Slovenia · Armenia

R.5 ratings

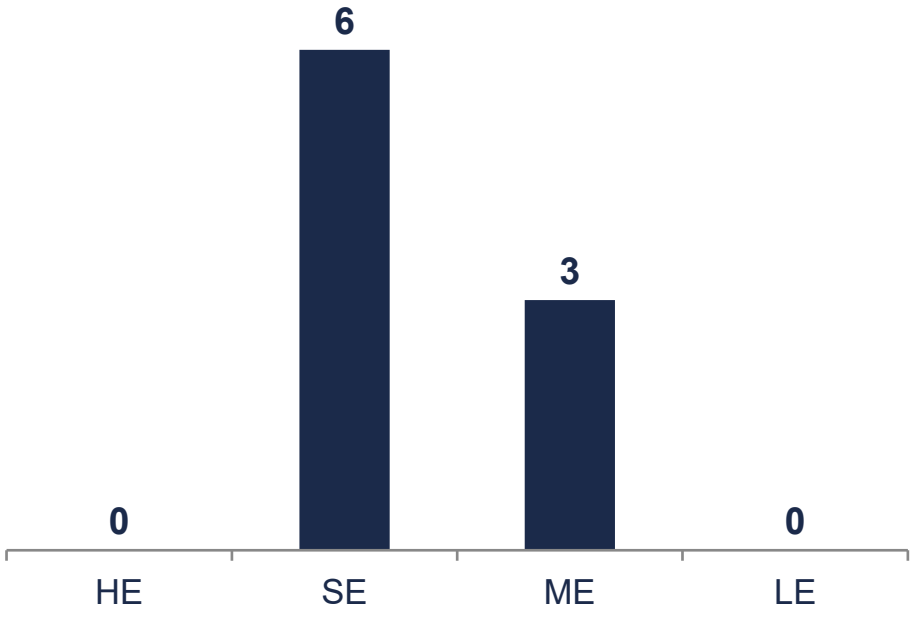
Jurisdiction	Assessor	Published	R.5
Belgium	FATF	Dec 2025	**C**
Malaysia	FATF/APG	Dec 2025	**C**
Italy	FATF	Apr 2026	**C**
Austria	FATF (IMF)	Apr 2026	**C**
Singapore	FATF/APG	May 2026	**LC**
Latvia	MONEYVAL	Feb 2026	**LC**
Serbia	MONEYVAL	Apr 2026	**LC**
Slovenia	MONEYVAL	Jul 2026	**LC**
Armenia	MONEYVAL	Jul 2026	**LC**



TC is necessary, not sufficient for effectiveness

	SE	ME
R.5 C	Belgium Malaysia Italy Austria	— (none)
R.5 LC	Singapore Latvia	Serbia Slovenia Armenia

IO.9 Outcomes



Prosecution volume does not decide the rating: Latvia reached SE with zero prosecutions; Slovenia reached ME with 16 pre-investigations.

Jurisdiction	IO.9	TF prosecutions / convictions (as reported)
Italy	**SE**	Significant number of complex stand-alone cases; high conviction success
Malaysia	**SE**	7 convictions since 2019 (none in 2015 MER)
Austria	**SE**	Substantive number of investigations and prosecutions, in line with risk
Singapore	**SE**	6 prosecutions, one typology
Belgium	**SE**	Operational CFT strategy covering all targets
Latvia	**SE**	No prosecutions; disruption measures applied
Serbia	**ME**	Limited investigations, partly reflecting risk
Slovenia	**ME**	16 pre-investigations, all dismissed
Armenia	**ME**	1 investigation, no prosecutions

Best practices

Italy

FIU-led TF analytics

Sophisticated analysis of TF-related STRs by UIF and Guardia di Finanza produced a significant number of complex stand-alone TF investigations; prosecutors generally secure convictions.

Malaysia

Centralised TF investigation

TF investigations centralized in the **Police Special Branch** since 2015 — from zero cases to seven convictions.

Latvia

Dedicated CFT Task Force

FIU-led task force (State Security, central bank, Customs, SRS) analyses flows to high-risk jurisdictions, monitors legal persons with high-risk BOs, and refers suspicions.

Latvia

Disruption in lieu of conviction

Alternative measures actually applied in practice; clear understanding that intent is proven from objective facts.

Austria

Risk-consistent caseload

Substantive number of investigations and prosecutions against small-scale TF typical of the country's risk profile.

Slovenia · Singapore

Fast intelligence-to-police pipeline

OMLP prioritises TF STRs for timely police dissemination; Singapore actively uses financial intelligence in TF investigations.

Sources: FATF MER pages (Italy, Malaysia, Austria, Singapore); MONEYVAL MERs (Latvia, Slovenia).

Shortcomings flagged in SE-rated jurisdictions

Belgium	TF not formally integrated into the CT strategy or into the operational handling of TF cases; TF experts should work more closely with terrorism experts.
Malaysia	Dissuasiveness of sentences (1.5–6 years) questioned; conviction rate still low relative to risk.
Italy	Simple cases — self-funding or low-value transfers — are not pursued with a view to prosecution.
Austria	Networks involving NPOs, legal persons and hawala-type schemes under-investigated; no legal basis for real-time surveillance of encrypted communications.
Singapore	All six prosecutions share one typology; no CTF activity on funds transiting via banks or DPTSPs — a risk Singapore itself rates among its highest.
Latvia	No prosecution or conviction, so no case law on the evidence needed (offset by disruption and risk context — no KRA).

Why three MONEYVAL members stayed at moderate

Serbia · IO.9 ME

- Limited investigations, only partly reflecting the risk profile
- High evidentiary requirements
- No strategic coordination
- KRA: comprehensive operational approach and strategy

Slovenia · IO.9 ME

- Proactive identification rare — no systematic OSINT or strategic analysis
- Pre-investigations since 2020 all dismissed; no prosecutions
- CT strategy not informed by TF investigations
- KRA: proactive identification, OSINT, monitoring of TF trends

Armenia · IO.9 ME

- TF from other criminality and high-risk-country transactions not explored
- Private-sector underreporting of TF
- One investigation, no prosecutions
- Alternative measures available but never used

lessons for jurisdictions preparing an on-site

Latvia — SE

Zero prosecutions · low risk · risk well evidenced · disruption applied in practice · intent standard understood

Slovenia / Armenia — ME

Zero prosecutions · low risk · risk inferred from absence of attacks · disruption unused or undocumented · reactive detection

1. **Proactive detection**
   TF identification beyond STRs: OSINT, strategic analysis, non-terrorism crime, HRJ
2. **TF typologies**
   Cases covering both simple self-funding and complex, network, NPO and transit flows. TBTF
3. **Documented disruption**
   A case file showing alternative measures actually applied where conviction is impracticable.
4. **Evidenced TF risk**
   Risk understanding built on data, not on the absence of attacks.
5. **Strategic approach**
   TF embedded in CT strategy, and investigations feeding back into it.



Example: Turkey MER

Turkey

13. FIs and VASPs have a generally strong understanding of the ML risks they are exposed to and the main ML risks identified by FIs and VASPs are generally in line with the findings of the NRA. Understanding of TF risks is more uneven. While banks - representing more than 75% of the sector - demonstrated a good understanding of TF risks, other FIs and VASPs have a more limited understanding, mainly considering TF risks in the scope of TFS. Overall, FIs and VASPs have a thorough knowledge of their AML/CFT obligations. Reporting entities apply mitigating measures, in particular CDD and take measures to identify beneficial owners. General reporting of suspicion from the highest risk sectors (banking, MVTS and VASPs) is substantial, while it is low for other FIs. Yet there is an overall limited number of TF STRs across all sectors, in particular for exchange offices, MVTS, and VASPs. PEP identification and monitoring is only partially effective, particularly among the largest group of exchange offices, which suggests constraints in TF detection and reporting relative to their assessed risk exposure.

8. Türkiye has identified ML/TF risks across DNFBP sectors through a comprehensive risk assessment. Despite some positive steps taken by competent authorities, DNFBPs' understanding of ML/TF risks remains limited. In the DPMS and REAs sectors, the understanding of ML risks is more developed, especially for larger entities, while TF risk understanding is limited to awareness of TF related TFS obligations. Accountants, lawyers and notaries have a more limited understanding of ML/TF risks.

FATF

FATF REPORT

Comprehensive Update on Terrorist Financing Risks



July 2025

TF Materiality Factors

1. **Territorial control**
   Areas held by terrorist groups enable taxation, extortion & humanitarian aid exploitation

2. **Armed conflict proximity**
   Conflict zones offer weak oversight and access to looted or diverted assets

3. **Natural resource access**
   Control of oil, gas, minerals & agriculture generates illicit revenue streams

4. **Weak governance & corruption**
   Compromised institutions reduce detection and enforcement capacity

5. **Porous borders**
   Cross-border smuggling of cash, goods & people funds operations

6. **Informal & cash-based economies**
   Unregulated, cash-heavy sectors mask the origin and movement of funds

7. **State sponsorship**
   External state support supplies funding, materiel & safe haven

8. **Free trade zones**
   Reduced customs scrutiny facilitates trade-based value transfer

How Funds Are Raised, Moved & Managed

Cash

Remains dominant, especially in conflict zones & remote areas with limited financial infrastructure

MVTS / Hawala (HOSSPs)

Unlicensed remittance & hawala providers, now adopting blockchain-based transfers

E-money

Mobile money & online payment services, attractive in laxly regulated jurisdictions

Traditional financial services

Deposit accounts, wire transfers & prepaid cards, despite improved verification

Digital platforms

Social media, messaging apps & crowdfunding, especially with integrated payments

Virtual assets / VASPs

Growing use with obfuscation techniques and shift to privacy-focused alternatives

Legal Entities, NPOs, “humanitarian aid”

Abuse of legal entities & NPOs

- Shell companies & trusts move or launder funds across borders
- Sham NPOs created for fundraising, recruitment & logistics
- Legitimate NPOs abused without their knowledge
- Cash-intensive legitimate businesses generate revenue for TF in areas of control

Natural resources & criminal proceeds

- Oil, gas, agriculture, wildlife & precious metals trade and trafficking
- Extortion, taxation-like activity & coerced fees in controlled territory
- Kidnapping for ransom as a direct revenue source
- Human trafficking, migrant smuggling & trafficking of goods, drugs and arms

Priorities for jurisdictions, the private sector & the FATF Global Network

1

TFS

Coordinated, multilateral response; prioritise UNSC designations alongside UNSCR 1373 mechanisms

2

MVTS, VASPs & legal persons

Focus on high-risk areas: MVTS, VASPs & legal persons to close regulatory gaps

3

Outreach to uncovered sectors

Engage social media & messaging platforms via targeted public-private partnerships

4

CFT technical assistance

Embed CFT priorities in broader capacity-building & Global Network cooperation

5

Enhance private-sector support

Centralised repository, targeted communications & in-person/online training

6

Humanitarian activity

Ensure CFT measures do not impede lawful, impartial humanitarian operations

Lessons for Malta

1. **Update NRAs sectoral & Business TF Risk assessments**

   Reflect current TF typologies — VAs, social media, e-money

2. **Refresh red-flag indicators**

   Incorporate indicators across customer, transaction & geographic categories

3. **Prioritize MVTS, VASP & NPO supervision**

   These remain the highest-exposure sectors per this report

TERRORIST FINANCING TYPOLOGIES

EU TE-SAT 2026 · Europol Terrorism Situation and Trend Report

Funding, movement, and organised-crime nexus patterns observed across the EU in 2025



Three typology categories

TE-SAT 2026 groups terrorist-financing methods by function: how funds are collected, how they are moved and stored, and where financing overlaps with organised crime

13

Collection

Methods used to raise funds — from salaries and donations to fraud, extortion, and misuse of benefits.

5

Movement & Storage

Methods used to transfer or hold funds — hawala, couriers, bank transfers, crypto, in-game value transfers.

1

Nexus with Organised Crime

Overlap between terrorist actors and criminal networks — money laundering, weapons and drug trafficking.

How funds are raised (I)

- **Salaries & legitimate income**

  Cited EU-wide for jihadist and left-wing/anarchist actors; left-wing financing relied largely on personal income.

- **Membership fees**

  Recurring funding source across right-wing, left-wing/anarchist, and ethno-nationalist (PKK) networks.

- **Donations & crowdfunding**

  Jihadist and PKK networks used donations and crowdfunding. France, 1 Apr 2025: woman arrested for financing jihad-related travel.

- **Propaganda material & merchandise**

  Sale of propaganda, merchandise, accessories and literature — reported across right-wing and left-wing/anarchist networks.

- **Event entry fees & fundraising events**

  Entry fees and fundraising events recur across right-wing, left-wing/anarchist, and PKK financing models.

- **Theft**

  Listed among general terrorist-financing collection methods and among jihadist funding sources.

How funds are raised (II)

- **Illicit goods, incl. drugs**

  General TF typology; jihadist funding sources include drug sales.

- **Fraudulent NGOs & charitable fronts**

  Fraudulent NGOs and charitable fronts used by jihadist and PKK networks; some donor funds diverted abroad without donors' knowledge.

- **Fraud**

  A jihadist funding source; PKK fundraising also associated with fraud, laundering and extortion.

- **Social benefits & loans**

  Jihadist funding may draw on legitimate income, loans, and social benefits.

- **Coerced contributions & extortion**

  PKK financing includes coerced contributions and extortion; dissident republican groups engage in extortion, smuggling and protection activity.

- **Misuse of government grants**

  Left-wing/anarchist actors misused governmental financial support allocated to legitimate foundations and associations.

- **Structured commercial fundraising**

  PKK financing assessed as structured and transnational, including the annual 'Kampanya' campaign and commercial fundraising via associations and media.

How funds are moved and held

- **Hawala systems**

  A traditional TF movement channel; hawala providers increasingly add online services. Used in jihadist transfers.

- **Cash couriers**

  A recurring general and jihadist transfer method; PKK financing also uses cash couriers alongside legal and illegal channels.

- **Bank transfers & money transfer services**

  Jihadist funds moved through conventional bank transfers and licensed money transfer services.

- **Cryptocurrencies**

  Growing use for movement and storage. Germany, sentenced 6 Mar 2025: individual transferred ~USD 1,676 in crypto to support IS while planning to join ISKP.

- **Value transfers via online games**

  An emerging technology-enabled channel for moving or storing value, alongside cryptocurrencies.

Nexus with Organized Crime

Money laundering, weapons and drug trafficking

Some terrorist actors engage directly in organised crime, or cooperate with criminal networks, through money laundering, weapons trafficking, or drug trafficking. PKK-related networks show indications of links to organised crime, including drug-trafficking connections.

Why this matters for AML/CFT

The organized-crime nexus means AML controls built for predicate crimes — trafficking, fraud, extortion — carry direct CFT relevance. Typology overlap complicates STR/SAR triage and requires joined-up ML/TF risk assessment.

2025 case examples cited in TE-SAT

France

1 April 2025

DONATIONS / CROWDFUNDING

A woman was arrested for financing a friend engaged in jihad-related activity in Syria.

Finland

4 November 2025

STRUCTURED COMMERCIAL FUNDRAISING

Three men were arrested for collecting money on behalf of the PKK.

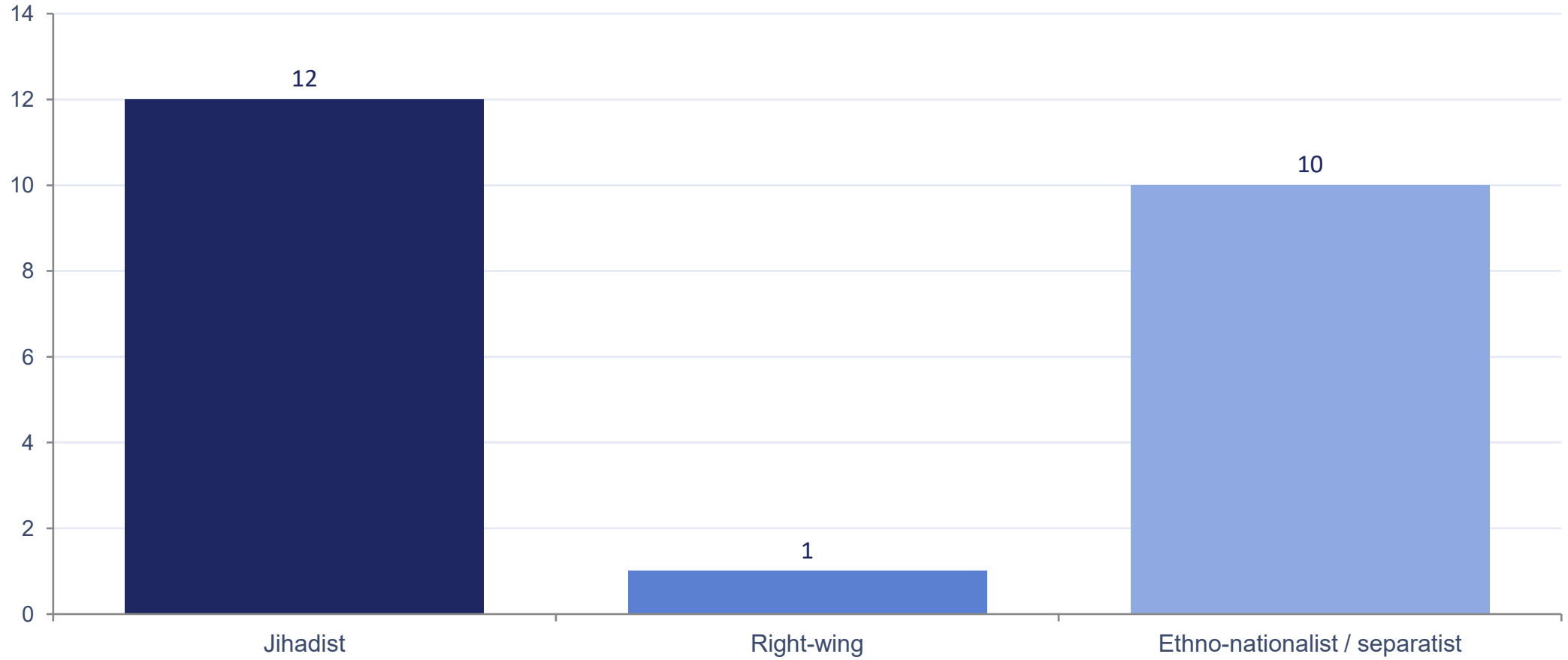
Germany

Sentenced 6 March 2025

CRYPTOCURRENCIES

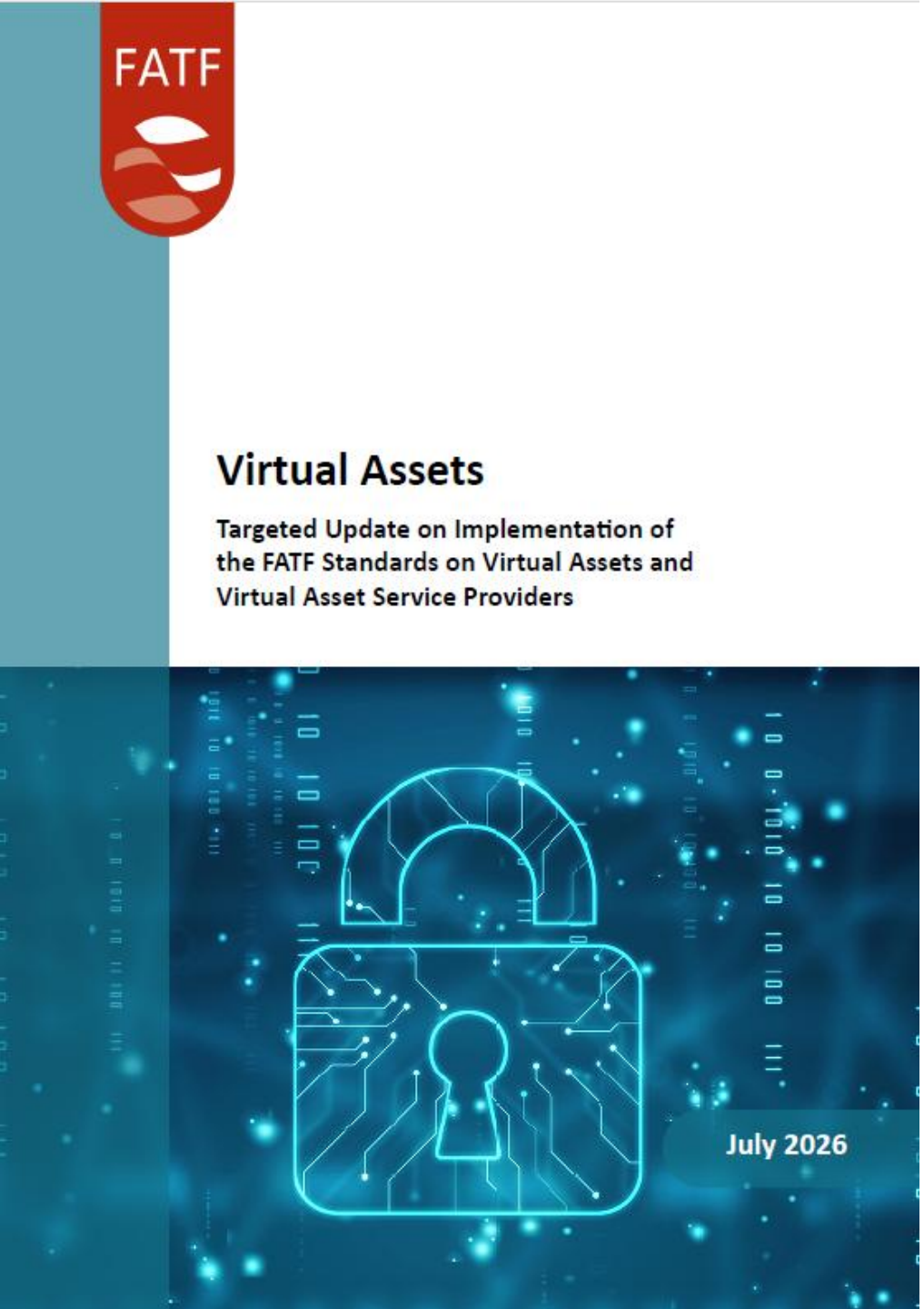
An individual transferred roughly USD 1,676 in cryptocurrency to support IS while planning to join ISKP.

TF-specific arrests by actor type, 2025



KEY TAKEAWAYS

1. TF collection methods remain diverse and largely low-value, ranging from lawful income to fraud and extortion — favouring a broad-spectrum monitoring approach over reliance on any single red flag.
2. Hawala, cash couriers, and increasingly crypto and in-game value transfers coexist as movement channels — sanctions and transaction-monitoring coverage should span both formal and informal rails.
3. The organised-crime nexus (PKK/drug trafficking; laundering-extortion links) means predicate-crime typologies used in ML risk assessments carry direct CFT relevance and should not be assessed in isolation.
4. 2025 EU arrests were concentrated in jihadist (12) and ethno-nationalist/separatist (10) categories — a useful prioritization signal for jurisdiction- and sector-specific risk assessments.



FATF’s recent report focuses on stablecoins and un hosted Wallets

Terrorist organizations, including ISIL and Al-Qaeda, increasingly favor stablecoins over Bitcoin, exploiting rotating wallet addresses, micro-splitting of funds, and multi-hop transfers through VASPs and over the counter brokers with minimal CDD requirements, while further pairing stablecoins with decentralized finance tools and unhosted wallets to circumvent compliance controls.

CTF preventative measures

Inherent risk

Controls

STR Quality

STR / TFS coordination

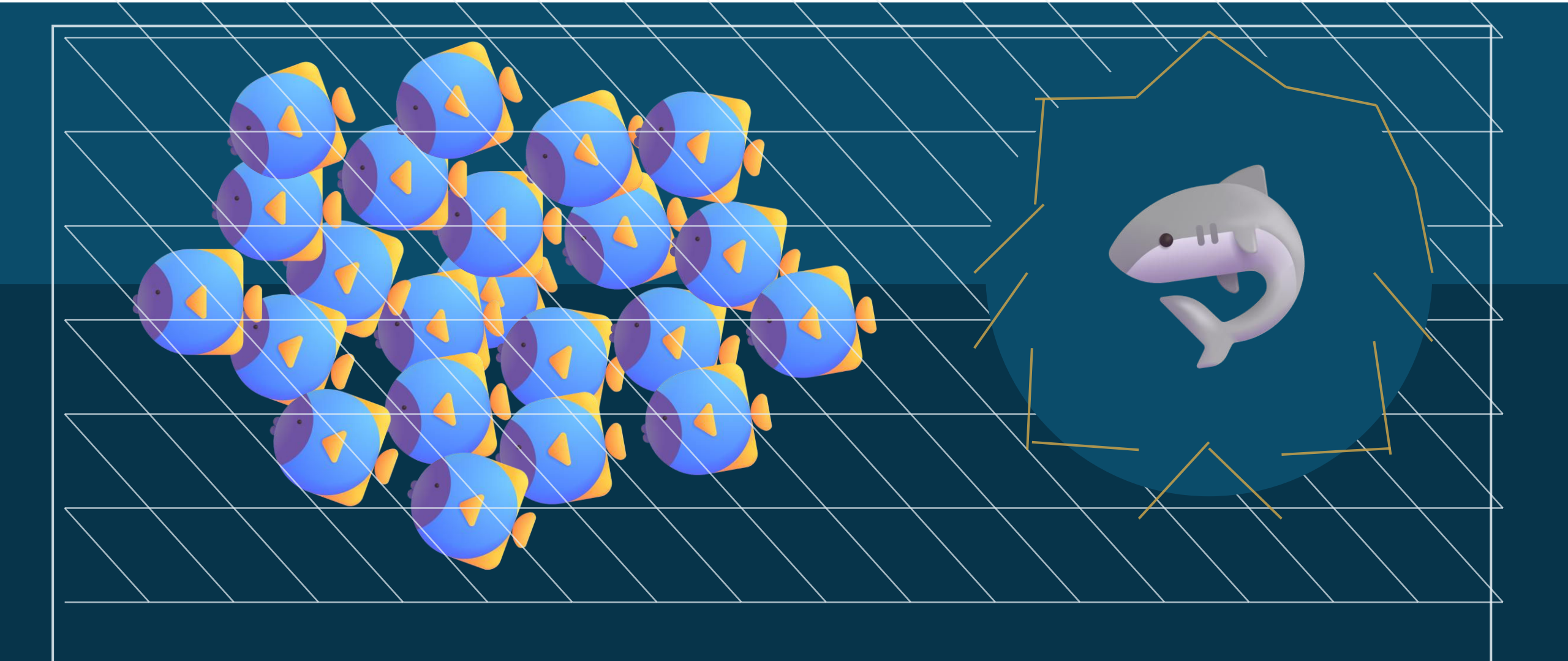
TF Conclusions

- Properly Understanding the TF Risk - not just about financing Terror Attacks, it is mainly about providing support for terrorist organisations
- Focusing on all relevant types of TF (e.g. TBTF, not over focusing on FTF)
- Taking R.5 seriously – (e.g. is providing humanitarian aid through a terror organization or to an individual terrorist=TF)

- All International Financial Centres are vulnerable for TF abuse as a “flow through” jurisdiction.
- Things to look out for:
  - Jurisdictional risk
  - Abuse of NPOs, Legal entities, and complex structures
  - Check your customer base for TFS and other Sanctions regimes
  - Crypto
- Emphasis is on where the money is going to
- Need for Strategy led enforcement effort (interagency national and international cooperation)

- Limited success in criminal proceedings (compared to reality i.e. Panama papers)
- Preventative measures sometimes successful
  - More against fighters (ISIS)
  - Less against Terrorist organizations (Afghanistan, Middle east)
  - Less against state sponsored (Iran, PA)
- Success in civil law suits (victims)
- NPO (cash, De risking?)
- MVTS – for ML purposes as well

The AML/CFT Net



Thank you !

Yehuda Shaffer
yshaffer@riskbasedconsultancy.com