PST

National Risk Assessment (NRA) Terrorist Financing 2026

Document date, 24 June 2026

Contents

1 Background....4

2 Methodology and data sources....5

PST's mandate and definitions 7

3 Terrorism threat landscape 8

Threat landscape for terrorist financing 8
Drivers of terrorist financing....10
Scale of terrorist financing in and from Norway 12

4 Selected indicators and methods of terrorist financing 14

Extreme views and links to extremist networks 15
Benefit claimants 15
Links to criminal networks....15
Minors and young adults....16
Concealed ownership and beneficial owners 19
Exploitation of business structures 19
Charitable organisations 21

5 Selected assets used for terrorist financing....22

Cash 22
Cryptoassets....23
Prepaid cards....25
Gold and luxury goods....25

6 Selected obliged entities at particular risk of exploitation for terrorist financing 26

Banks 26
Payment services 27
Cryptoasset service providers 29

7 Illegal and unregulated activities 30

Illicit payment intermediary services 30
Professional enablers 31
Raising funds and other assets 32
Social media, digital platforms and gift cards 34
Gold dealers 35
Gambling and gaming 35

8 Vulnerability landscape 37

Available methods and capacity 38
Other vulnerabilities of the Norwegian framework 38
State actors 40

9 Consequences 40

10 Overall risk assessment 41

Appendix 42

Section 135. Terrorist financing 42
Section 136 a. Penalty for participation, etc. in a terrorist organisation 42

Executive summary

Actors who facilitate terrorism pose a major threat to international peace and security. Terrorist financing is a complex global phenomenon that contributes to the terrorist threat. The terrorism threat landscape is shaped by the current global situation, which increases the opportunities available to extremist actors. Geopolitical shifts and technological advancements are creating new channels for financing terrorist activity. These developments make it more difficult for obliged entities and security services to prevent and disrupt terrorist financing.

The scope and size of contributions from Norwegian extremists to international terrorism are limited, and domestic actors generally lack the capacity to raise substantial funds. At the national level, terrorist financing primarily takes place through lone actors with limited financial resources, whose support is often aimed at specific individuals or purposes rather than organised networks.

The report demonstrates that terrorist financing utilises diverse channels, leveraging assets like cash, crypto, prepaid cards, gold and luxury goods, whilst also exploiting unregulated activities and digital platforms. Banks, payment services, cryptoasset service providers, fundraising activities and professional enablers can be particularly vulnerable to exploitation. Impressionable children and adolescents, companies with opaque ownership structures and links to criminal networks are also sources of increased vulnerability.

The overall risk of terrorist financing is assessed as MODERATE. While the actual scope appears to be limited, existing vulnerabilities and the potential for exploitation mean that the risk cannot be considered LOW. The risk of domestic terrorist

1 Background

Actors who facilitate terrorism pose a major threat to international peace and security. Terrorist financing is a complex global phenomenon that contributes to the terrorist

threat. A common feature of terrorist financing is the exploitation of international transfer systems to fund terrorist attacks or the activities of terrorist organisations.

Preventing terrorist financing helps combat terrorism and reduce the threat. Countering the financing of terrorism is therefore a high international priority, in line with the priorities of the Financial Action Task Force (FATF), the United Nations (UN) and the European Union (EU).

> *'Terrorist activity is a particularly serious form of crime because it threatens the fundamental safety and freedom of citizens. […] If we can prevent and disrupt the flow of funds for terrorist activity, we can also prevent terrorist attacks.'*
>
> - The Norwegian government's strategy for combatting money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction
>
> (June 2020)[1]

As with the National Risk Assessment (NRA) of money laundering, the NRA of terrorist financing is intended to serve as a key knowledge base for developing a shared understanding of terrorist financing risks in Norway. The purpose of the assessment is to support a risk-based approach to countering the financing of terrorism.

2 Methodology and data sources

The Ministry of Justice and Public Security commissioned the National Police Directorate and the Norwegian Police Security Service (PST) to prepare the 2026 NRA. The National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) was responsible for preparing the money laundering section of the NRA and PST was responsible for the section on terrorist financing. The 2026 NRA is published in two parts, which should be read in conjunction with one another. Several factors associated with money laundering will also be relevant to terrorist financing, even if they are not explicitly mentioned here.

The methodology is based on an analysis and assessment of three factors derived from FATF:[2] threat, vulnerability and consequence. Certain adjustments have been made to account for the differences between money laundering and terrorist financing

[1] Regjeringen.no, The Norwegian government's strategy for combatting money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction, June 2020

[2] The methodology is detailed further in the 2026 NRA of money laundering by Økokrim, and described in more detail in FATF's Terrorist Financing Risk Assessment Guidance.

and the specific conditions in Norway. For example, the report makes limited reference to geographical risk factors. These risks are dynamic and must be understood in terms of the financial flows[3] of individuals seeking to finance terrorism.

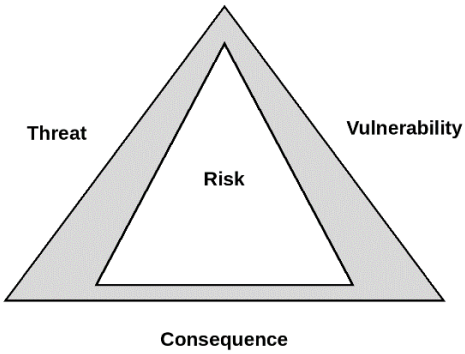


Figure 1: Risk assessment model, Økokrim

The risk assessment seeks to highlight which activities are considered to pose a risk of terrorist financing. Risk is assessed according to a scale consisting of four levels: low, moderate, significant and high.

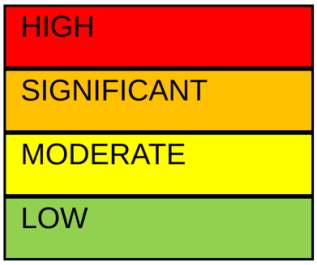


Figure 2: Risk assessment scale with colour coding

As with the NRA of money laundering, PST's assessment builds on the 2022 NRA and is therefore limited to the most relevant and prominent risks. Consequently, the assessment does not cover all potential risks that may need to be considered; it focuses instead on areas identified by PST during the reference period 2022–2026, based on the current knowledge base.

The data and information underpinning PST's assessment are derived in part from its intelligence-gathering activities, external specialists and public agencies. The information presented in the report is limited due to security classifications. Additional vulnerabilities are detailed in Chapter 8.

Terrorist financing is inherently transnational. Based on the available data, this report will include some phenomena and methods that have not been directly observed by

[3] In the context of terrorist financing, a financial flow is the movement of economic value from a source to an end purpose, in the form of money, goods, services, or other assets.

PST in Norway but are nevertheless considered relevant and within the scope of possible terrorist financing in and from Norway.

In recent years, PST has seen an increase in the amount of intelligence relating to terrorist financing. Throughout the reporting period, there has been a steady rise in reports of suspected terrorist financing from the public, as well as from domestic and international partners. Although the overall evidence base remains limited, the rising number of reports indicates a heightened focus among obliged entities[4] and the authorities. In the long term, this growing volume of information will strengthen efforts to counter the financing of terrorism.

PST's mandate and definitions

PST's duties and responsibilities in relation to terrorist financing are set out in Section 17b of the Norwegian Police Act. PST is responsible for preventing and investigating offences under Sections 135 and 136a of the Penal Code. Section 17g of the Police Act further provides that the head of PST may order the freezing of assets where there are reasonable grounds to believe that an individual has attempted to commit or has committed a specified terrorist offence.

In this report, the term ***terrorist financing*** is used as defined in Section 135 of the Penal Code. Section 136a also covers terrorist financing. The concept of terrorist financing encompasses a wide range of activities.

Probability refers to a set of standardised probability terms used by PST.[5] The purpose of these terms is to ensure a uniform description of probability in assessments and thereby reduce ambiguity and misunderstandings.

The term ***terrorist threat*** refers to the overall terrorism threat landscape. While probability terms represent PST's assessment of the likelihood of an attempted terrorist attack, the terrorist threat level reflects the severity of the situation.[6]

---

[4] Throughout this risk assessment, solicitors, banks, accountants, estate agents and other professionals are referred to as 'obliged entities'. The term denotes entities subject to Norway's Anti-Money Laundering Act that are legally required to report suspicious transactions to Økokrim.

[5] See the description of probability terms in the National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

[6] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

Extremism means acceptance of or support for the use of violence to achieve political, religious or ideological objectives.[7]

Vulnerability refers to factors that can be exploited by threat actors or that can support or facilitate such activity. Vulnerabilities can include characteristics of a particular sector, financial product or type of service that make them attractive for terrorist financing. They can also include weaknesses in measures specifically designed to counter the financing of terrorism, or features of a jurisdiction that may make it easier to raise or transfer funds, such as a large informal economy or lack of border controls.[8]

Consequence refers to the harm or impact that terrorist financing can cause if it materialises. This encompasses the effects on financial systems and institutions, as well as broader consequences for the economy, society and national interests. The consequences of terrorist financing are generally considered more severe than those of money laundering and other types of economic crime.[9]

3 Terrorism threat landscape

Threat landscape for terrorist financing

Organised terrorist activity often requires cross-border financing. The terrorism threat landscape is shaped by a range of factors that create different opportunities, some of which are highlighted in PST's National Threat Assessment (NTA).

Geopolitical tensions create new opportunities for terrorist financing

Geopolitical tensions, uncertainty and destabilisation often lead to power vacuums, weakened state institutions and heightened social unrest. These in turn create favourable conditions for insurgent groups, non-state armed actors and violent extremists.

Several regions are currently characterised by great power rivalries, the erosion of international norms and growing instability. Conflicts in the Middle East and Africa have created conditions that terrorist groups have exploited for radicalisation and

[7] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

[8] FATF, Terrorist Financing Risk Assessment Guidance, 2019

[9] FATF, Terrorist Financing Risk Assessment Guidance, 2019

recruitment, and to expand their terrorist and financing activities both locally and in the West. Economic and social unrest in these areas makes it easier to recruit members for terrorist activity, including terrorist financing, and to raise funds from local populations and exploit resources in areas under their control. Great power rivalries and proxy conflicts can also lead to the emergence of different factions, enabling insurgent groups to gain access to resources and legitimacy that they would otherwise not have. Competition for natural resources can further expand the opportunities available to terrorist actors, as deprivation and resource shortages create desperate conditions that terrorist groups can exploit for recruitment, seizing power and gaining strategic control over resources.

Meanwhile, conflicts and humanitarian crises often lead to increased use of cash and informal money transfer services, making financial flows more difficult to trace. Geopolitical tensions can also contribute to the misuse of foreign aid, charitable donations and diaspora remittances, while digital platforms and social media make it easier to mobilise support across borders.

In addition, sanctions, disruptions to trade and international divisions can create more grey areas, where illicit networks have greater scope to operate. Overall, therefore, geopolitical tensions not only increase the risk of terrorism, but also strengthen the financial structures that enable terrorist activity.

Grey-zone activities complicate the threat landscape

The threat landscape is further characterised by multiple actors with different motivations who increasingly appear to cooperate, including state actors, terrorist groups and actors involved in organised crime.[10] This development is blurring traditional distinctions between different types of crime. In line with observations made by FATF and Europol, we are also seeing evidence in Norway that a number of extremists have links to state actors, criminal networks and groups involved in activities such as money laundering and various predicate offences. This makes the threat landscape more diffuse and complex, as it can be difficult to distinguish between terrorist financing and other forms of criminal activity.

Use of intermediaries to conceal transfers or circumvent legal restrictions is increasing, making it more difficult to uncover potential terrorist activity and terrorist financing and to prove that funds were knowingly provided for terrorist purposes.

[10] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

Use of artificial intelligence creates opportunities

Digital innovation and new technological solutions for value transfers, together with the growth of artificial intelligence (AI), have further contributed to the increasing complexity of transaction flows. This, in turn, has expanded threat actors' ability to operate covertly, particularly where transactions are fragmented and occur rapidly between different financial systems and jurisdictions.

Europol highlights how AI and other emerging technologies are creating new opportunities, by making terrorist financing cheaper, faster and more adaptable. AI can also make illicit financial flows appear legitimate. This includes the use of false identities, manipulated documents and virtual assets, as well as the production of high-quality forged documents, concealment of senders and recipients, and the use of sophisticated payment instructions.[11]

AI also lowers the threshold for digital influence and social manipulation, increasing the risk of more targeted content, cheaper production of propaganda and more effective mobilisation of potential supporters.[12] Such communication also increases the risk of terrorist financing, for example by encouraging money transfers in digital forums.

These factors are considered likely to increase the risk of terrorist financing both within Norway and from Norway to other countries.

Drivers of terrorist financing

Global developments point to a clear geographical and operational shift in the pattern of terrorist attacks. International analyses, including by Europol and the Institute for Economics and Peace,[13] indicate that the deadliest terrorist activity is increasingly concentrated in the Sahel region and parts of South Asia, while Europe and other Western countries are characterised by a more fragmented and less predictable threat landscape. In the West, there is a notable rise in threats posed by lone actors and small, loosely structured networks. These are often fuelled by rapid online radicalisation through closed online forums and social media.

---

[11] FATF, Horizon Scan: Artificial Intelligence and Deepfakes, 2025

[12] Europol, European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, 2025

[13] Institute for Economics and Peace, Global Terrorism Index 2026: Measuring the impact of terrorism, 2026

Overall, these developments indicate that the centralised capacity of traditional terrorist organisations has been weakened in several regions, while the threat landscape in Europe and other Western countries has become more decentralised, digitalised and difficult to detect at an early stage. A more fragmented threat landscape also aids the financing of terrorism through small, less conspicuous transfers, often using digital services, cryptocurrencies and cross-border transactions.[14]

Terrorist activity in Europe has surged over the last couple of years, reaching levels not seen for some time. However, most planned attacks are averted by security and intelligence services. Islamist extremist terrorist activity in Europe has increased considerably since Hamas' terrorist attack on 7 October 2023 and Israel's subsequent military operation in Gaza. The high level of terrorist activity continued in 2025 and is expected to persist in 2026. Right-wing extremist terrorist activity in Europe has remained at a stable level since 2020.

Europol reported that 449 people were arrested for terrorism-related offences in Europe in 2024, an increase compared with both 2023 and 2022. The largest proportion of arrests related to Islamist extremism (289), followed by right-wing extremism (47).[15] However, Europol's annual TE-SAT reports show that extremism in Europe is increasingly characterised by hybrid and ideologically diverse frameworks, with the traditional boundaries between jihadist, right-wing and other forms of extremism becoming increasingly blurred. Europol also highlights a concerning increase in the number of minors involved in terrorism-related offences, as well as the use of digital platforms and encrypted messaging applications for propaganda, recruitment and operational planning. Issues relating to minors are addressed later in this report.

According to the 2026 NTA, the terrorist threat level in Norway is assessed as MODERATE, meaning that PST's assessment is that one or more persons intend to carry out a terrorist attack but have not taken active steps or devised realistic plans to do so, and/or that there are no factors that heighten the terrorism threat. The terrorist threat level reflects the overall threat posed by all forms of ideologically, politically and religiously motivated violence.

---

[14] For further information on trends and indicators, refer to, for example, JRC Indicators Explorer, developed by the European Commission's Joint Research Centre, which assembles information from a range of sources, including the Global Terrorism Index.

[15] Europol, European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, 2025

PST assesses that Islamist extremists and right-wing extremists may continue to attempt to carry out terrorist attacks in Norway in 2026, and considers these groups to pose the most serious terrorist threat to Norway.[16]

All threat assessments are subject to inherent uncertainty, and the threat landscape is impacted by a number of factors. The NTA notes that, although the terrorist threat level is MODERATE, the terrorist threat landscape is more complex and unpredictable than before, with the threat heightened for certain groups that are particularly exposed.

Global unpredictability and uncertainty, linked to potential isolated events and longer-term negative trends, also lead to rapid changes in the overall situation. As described in the 2026 NTA, several other strands of extremism have also become prominent, including anti-government extremism. PST is aware of terrorist financing cases linked to these extremism currents in several countries, including in Europe.

The focus should therefore be on the risk of terrorist financing within the various strands of extremism, including in Norway.

Scale of terrorist financing in and from Norway

'We also expect that some individuals in Norway will provide financial support for terrorist activity abroad. PST has observed a growing number of cases in which funds are transferred abroad via online payment services, with some recipients suspected of supporting terrorism. Not all service providers have a duty to report to Norwegian authorities, and the payment services themselves are constantly evolving. We expect this trend to continue.'

- *National Threat Assessment 2026 (PST)*

The threat from Islamist extremists persists, despite few individuals in Norway being identified as supporters. Previously established groups remain largely inactive, but there are few indications that well-established extremists have been deradicalised.[17]

In Norway, there are few clear, openly visible extremist groups with a common objective operating in the physical or digital domain. However, many Islamist

[16] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

[17] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

extremists are connected through looser ideological networks or other forms of association. Several individuals in Norway also have links to European and other international Islamist extremist networks. These networks could potentially call on them to facilitate or carry out terrorist attacks, thereby constituting a risk of terrorist financing.[18]

In Norway, right-wing extremists operate in a small number of physical spaces and numerous digital spaces. These extremist groups vary in size, organisational structure, level of activity and ideological orientation, and several maintain links with like-minded groups in other countries. Alongside the physical spaces, a range of digital spaces exist where Norwegian right-wing extremists share ideology and propaganda.[19] Nevertheless, the absence of established right-wing extremist terrorist organisations limits these extremists' capacity to plan, finance and coordinate complex attacks.[20]

Despite the foregoing, PST is aware of instances during the reference period where funds have been transferred to finance terrorism, both in Norway and abroad. Based on the information currently available, terrorist financing is assessed to account for a small proportion of the Norwegian economy as a whole, both in terms of the number of transactions and the amounts involved.[21]

Transaction data held by PST show that funds are primarily transferred to terrorist groups abroad, including IS, al-Qaida, Hezbollah and al-Shabaab. The amounts are modest, and the transactions are spread over extended periods. There have also been instances of transactions being split between different service providers, as well as the use of intermediaries in other European countries.

Individuals affiliated with foreign terrorist organisations tend to receive the largest share of funding originating from Norway. These transfers are typically facilitated by networks operating across multiple European countries, who then forward the funds to other extremist facilitators located close to the terrorist organisations' main operational bases.

---

[18] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

[19] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

[20] The Norwegian Intelligence Service (NIS), Threat Assessment, Focus, 2026

[21] Økokrim, National Risk Assessment, 2026

Based on the available data, PST finds that funds or assets used to finance terrorism often originate from legitimate sources of revenue. Like extremists in other European countries, Norwegian extremists are largely self-funded. They use their own money to pay for travel, clothing and equipment in preparation for potential journeys to conflict zones or in connection with attacks in Norway.[22] Personal funds also include proceeds from the sale of personal assets and valuables, money from family, and loans.

In recent years, a small number of extremists have been found to be funding relatively complex attacks, mainly abroad but also in Norway. Gathering these funds and resources can take place over several years. A Norwegian example is Anders Behring Breivik, who spent several years acquiring materials to improve his operational capability, including chemicals, weapon parts and ammunition. The acquisition of these materials did not require significant capital, and the purchases were spread over several years. Another example is Arfan Bhatti, who assisted Zaniar Matapour in planning the terrorist attack on 25 June 2022, including by helping him to obtain weapons.

PST emphasises that the potential for terrorist financing appears to be greater than they have so far observed in practice, both in Norway and abroad. Based on the vulnerabilities identified, there is therefore a risk that the extent of terrorist financing in and outside Norway is underestimated, also in relation to Norway being used as a 'transit country' for transfers linked to terrorist financing.

However, in PST's assessment, the greatest risk is associated with terrorist financing from Norway to other countries. This is linked to the information PST possesses on the threat landscape in Norway.

4 Selected indicators and methods of terrorist financing

This section highlights selected indicators and methods based on PST's experiences during the reference period. The selection is based on a review of PST's information and observations and is not exhaustive. The chapter is solely intended to highlight

[22] Europol, European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, 2025

indicators and methods that warrant particular attention in the current threat landscape.

Extreme views and links to extremist networks

Developing extreme views is considered to increase the risk of financing terrorism. Extremist ideologies or radicalisation, whereby a person gradually changes their views and increasingly accepts or legitimises the use of violence, are therefore associated with an increased risk of supporting terrorist activity.

PST has found that people with such views also frequently establish links with extremist networks, both in Norway and abroad. Support for terrorism is often channelled through these networks rather than directly to terrorist groups or to countries where such groups operate.

Benefit claimants

We have identified a risk of benefit claimants with extreme views using their benefits to finance terrorism.

PST has also observed several cases in which people who have fraudulently obtained government funds, such as government loans, child support, unemployment benefit and work assessment allowance, are at greater risk of using this income to finance terrorism abroad. This has also been observed elsewhere in Europe, and FATF member countries report that extremists are becoming increasingly adept at evading taxes in order to maximise their welfare benefit payments.[23]

Links to criminal networks

Over the course of several years, FATF has highlighted links between criminal networks and terrorist financing. These networks have supported terrorist groups in various ways, including by providing funds for weapons and other equipment, forged travel and identification documents, and other resources that facilitate their activities.[24]

---

[23] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[24] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

PST has observed that Norwegian extremists exploit vulnerabilities in society to some degree and engage in criminal activity to generate income for various purposes, including the financing of terrorism.

PST has observed that extremists at risk of engaging in terrorist financing often have close ties to criminals and criminal networks that commit a range of predicate offences to generate financial proceeds, such as fraud. Methods include using intermediaries to obtain loans, with the funds immediately dispersed to different accounts to conceal the financial flow.

International sources note that right-wing extremists are less likely to engage in profit-motivated crime than Islamist extremists. PST does not have detailed information on the scope of criminal activity for the various strands of extremism in Norway, but the same appears to apply here.

Greater convergence between criminal networks and extremists can increase the risk of both intended and unintended terrorist financing. Such convergence gives extremists access to established sources of income, logistics and mechanisms for concealing the proceeds from organised crime. Through links to smuggling, drug trafficking, illicit arms trade, extortion and other illicit trade, terrorist groups can more easily raise funds, move assets and conceal their activities within established criminal structures. FATF highlights the convergence of terrorist financing and organised crime as a clear emerging risk. Europol also notes how some extremist networks combine legitimate and illicit sources of income, including links to organised crime, which makes their financing more robust, diversified and difficult to detect.

Minors and young adults

'The challenge of radicalisation among minors and young adults is expected to continue in 2026.'

- *National Threat Assessment 2026 (PST)*

The radicalisation of minors and young adults is a growing concern in Norway. Poor mental health and social exclusion are two key vulnerabilities. Increasing numbers of children and adolescents are becoming involved in extremist networks, particularly through digital platforms. The threat landscape is further complicated by the conflation

of ideology and a fascination with violence, which makes it more difficult to uncover potential terrorist acts.[25]

Minors are a vulnerable group. This is particularly the case in the digital space, where the boundaries between propaganda, a sense of belonging and financial support can easily become blurred, a trend further compounded by AI. Under such conditions, fundraising, micro-donations and other forms of financial support can easily be facilitated under the guise of normal online engagement.[26]

Europol reports a growing number of minors and young adults involved in terrorism and violent extremism. The same report also highlights how extremists generally adapt their content on the platforms used by young people and use algorithm-driven content and gaming platforms for recruitment and radicalisation.[27]

The growing use of AI also makes minors vulnerable to influence operations, recruitment and digital mobilisation through more targeted, personalised and continuous exposure. In practice, this means that AI cannot only make it easier to influence young people, but also to use them as donors, intermediaries or low-profile intermediaries in small-scale, digital and interconnected transaction flows.

[25] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

[26] Europol, European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, 2025

[27] Europol, European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg, 2025

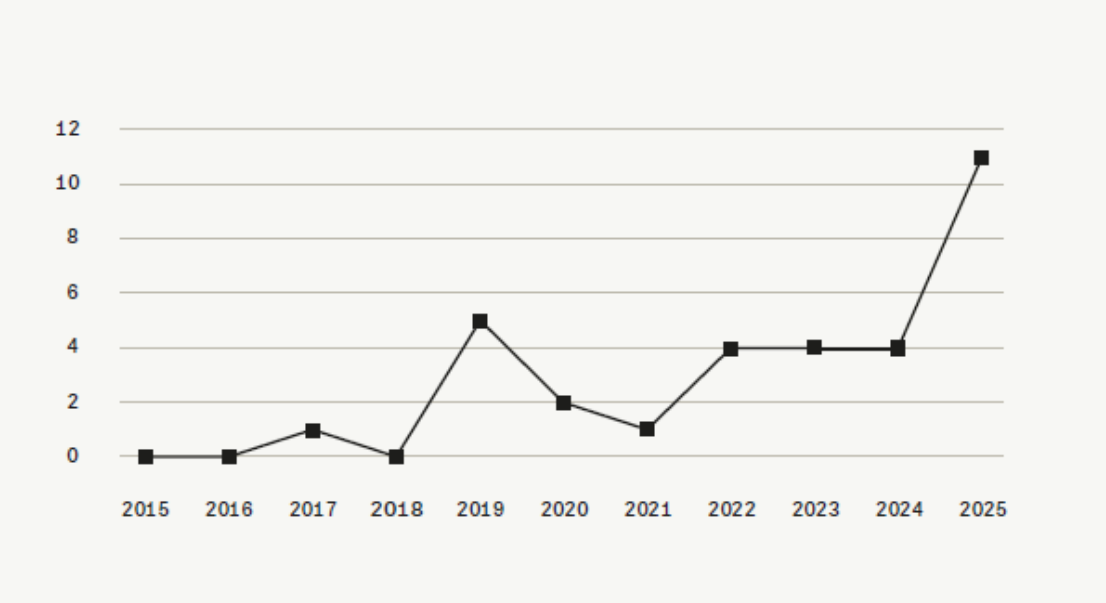


Figure 3: Trends in right-wing terrorist activity in the West involving minors in the period 2015-2025 (Source: PST)

PST, like the police more generally, has observed a rising prevalence of criminal activity among minors. This is consistent with the trend reported by Økokrim's Financial Intelligence Unit (FIU), which has observed a steady decline in the average age of people involved in suspicious activity (as per reports of suspected terrorist financing).[28]

PST finds that terrorist financing involving minors is particularly difficult to detect, as minors are often involved in cases where financial trails are weak, indirect or obscured through adults and digital intermediaries. This is consistent with findings from FATF, which notes that when younger people become involved in terrorism-related activity, income streams, bank accounts and transactions are less likely to be in their own names, making it more difficult to identify patterns and intervene at an early stage.

Although the security and intelligence services avert a large proportion of planned attacks, uncovering the plans of lone actors is still problematic.[29] The radicalisation of minors and young adults therefore remains a challenge for public authorities and obliged entities. Consequently, PST has reason to believe that the true scale is higher than reported.

---

[28] Økokrim, Financial Intelligence Unit Annual Report, 2025

[29] PST, National Threat Assessment 2026 (https://www.pst.no/wp-content/uploads/2026/02/National-Threat-Assessment-2026.pdf)

Concealed ownership and beneficial owners

PST is seeing more signs that extremists are learning how legitimate structures, such as businesses, associations and foundations, can be used to generate funds or conceal their intended use for terrorist financing.

PST has identified cases in which more complex corporate structures have been used to obscure transactions and recipients, and to conceal the identities of owners and beneficial owners. These corporate structures often span multiple jurisdictions and involve tax havens, countries with poorer compliance with international standards and regulations, the use of frontmen and front companies, and complex, fragmented or opaque supply or value chains.

Property is considered particularly well suited to concealing underlying ownership and beneficial ownership, through complex ownership structures and the use of blank deeds.

Similarly, investments in securities, funds or companies, and the establishment of corporate structures in jurisdictions with weaker oversight and less transparency, can be used to conceal the identities of the true investors, thereby generating seemingly legitimate income for obscured purposes

Exploitation of business structures

Extremists are increasingly found to be linked to other profit-generating criminal activity that is suitable for generating funds for terrorist financing. Refer also to the section on the use of cash in Chapter 5, as well as the chapter entitled ‘Exploitation of Business Structures’ in Økokrim’s National Risk Assessment (in Norwegian).

Industries with a risk of significant cash-generating activity, such as construction, retail, etc., are considered particularly vulnerable to exploitation for criminal purposes, and the proceeds can subsequently be used to finance terrorism. The vulnerability of an industry depends partly on the complexity of businesses, the opportunities for ‘unregistered employment’ (undeclared labour) and financial misappropriation that can generate large cash flows, the use of subcontractors or complex value chains, and cross-border geographic exposure.

Export of goods and services

The procurement of goods and services, including technology, weapons and other equipment, is essential to terrorist groups’ continued operations. Terrorist groups

have been found to obtain information, funds and necessary equipment by concealing support for their activities through the exploitation of businesses involved in the export of goods and services. This can occur through, for example:

- the use of front companies and frontmen to conceal the true purpose
- over/under-invoicing for traded goods or services
- fictitious exports
- trade in so-called 'dual-use goods'[30]
- the diversion of goods through jurisdictions with weaker controls and lower levels of regulatory compliance

Maritime transport, shipping, fisheries and other exporters are considered particularly suitable for concealing transactions and other assets intended to finance terrorism. Maritime transport and shipping often involve highly complex trade patterns and value chains. Businesses are also characterised by intricate ownership structures, operations in jurisdictions with weak state governance, and activities involving the movement of assets, including to higher risk areas.

It is also well established that the terrorist organisation IS has historically generated substantial revenues from oil and gas production and trade. The terrorist organisation al-Qaida is still actively trying to establish control over ports along the Gulf of Aden. The Yemeni Houthi movement has also sought to gain control of key oil and gas fields.[31]

Such terrorist organisations rely on partners to sell and transport these commodities, including logistics companies and intermediaries. Norway has a large oil and gas sector, supported by extensive logistics operations. Despite the strict regulation of the oil and gas industry on the Norwegian continental shelf, there is nevertheless a risk that Norwegian entities can be exposed, directly or indirectly, to financial flows used for terrorist financing.

[30] Dual-use goods are ordinary civilian goods, technologies or services that were originally developed for commercial purposes but also have properties that mean they can be used for military purposes.

[31] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

Sanctions evasion and terrorist financing risk

Many UN sanctions and restrictive measures imposed by the EU are targeted at terrorist organisations, individuals associated with them, or states that support such organisations. Sanctions evasion therefore entails a risk that funds may be transferred to actors engaged in terrorism. The methods used to evade sanctions often overlap with those used to conceal the fact that funds are intended for terrorist financing, such as the use of complex corporate structures, intermediaries and complex value chains. Involvement in sanctions evasion may therefore also amount to aiding and abetting terrorist financing.

Charitable organisations

Non-profit organisations (NPOs) transfer considerable amounts of money from Norway to organisations and entities abroad every year. Although many donations are intended for humanitarian purposes, those intentions may be exploited, resulting in funds being channelled into criminal activity, including terrorist financing.

Terrorist networks often exploit charitable organisations or establish fraudulent organisations to raise funds under the guise of humanitarian work. This has previously been seen, for example, in the cases of the Holy Land Foundation and the Global Relief Foundation, both of which were engaged in terrorist financing and were shut down following the 9/11 attacks in New York. Terrorists are also known to have used such organisations to transfer funds, provide logistical support, recruit members, gain legitimacy or otherwise support terrorist activities. PST is aware of cases in which extremists have established organisations in Norway with unclear purposes, where it is difficult to determine how funds and other assets raised have been used.

Oversight of the NPO sector largely depends on the extent to which organisations are registered, and those that are not included in public registers are subject to fewer oversight mechanisms. Organisations that deliberately avoid multiple registers and reporting requirements may have an underlying motive to limit scrutiny by the authorities.

The data show that NPOs with limited inclusion in registers, for example only in the Central Coordinating Register for Legal Entities, and whose primary purpose is to raise funds for conflict zones, pose the highest risk of funds being misappropriated for criminal purposes. These organisations are often subject to less stringent requirements and supervision, making them attractive to actors seeking to conceal terrorist financing.

5 Selected assets used for terrorist financing

Several financial flows are particularly vulnerable to being used for terrorist financing in and from Norway. Cash continues to play a key role and is often moved through informal channels and criminal networks, while cryptocurrencies are increasingly being used to transfer and conceal funds. Prepaid cards and trade in gold and luxury goods provide alternative channels, as these items are easy to transport and sell and difficult to trace. The funds in these financial flows are used to cover operational costs, support members and their families, and sustain the activities of extremist organisations.

This chapter presents a selection of financial flows that PST considers pose an elevated risk of terrorist financing. The list is not exhaustive but covers selected channels in Norway, based on the information available during the reference period. Reference is also made to the Norwegian Customs' analyses of payment flows and economic activity in the period 2022–2025 in the NRA of money laundering, including concealed financial flows, which are also relevant to the risk of terrorist financing.[32]

Cash

Cash is still considered one of the preferred methods for extremists to acquire, move, store and use funds anonymously.[33] In most cases, funds intended to finance terrorism are ultimately converted into cash to enable the anonymous payment of logistical and operational expenses, such as wages, equipment procurement and financial support for families.

Cash plays a central role in informal economies and organised crime networks. We have observed that some terrorist groups share transport routes with organised crime groups because these channels are ideal for concealing both the origin and

[32] Økokrim, National Risk Assessment, 2026

[33] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

destination of funds. Criminal migration routes and goods transportation networks can be used for discreet transactions in exchange for cash.[34]

Unlike the section on money laundering in the NRA, where cash is considered impractical in some respects, this is not the case with terrorist financing, which often involves smaller amounts that are easier to transport and sell. Cash is also preferred by a number of international terrorist organisations.

The data available to PST indicate that cash remains the dominant means of financing terrorism, partly because terrorist organisations often carry out terrorist activity in or are based in areas with less developed financial and digital infrastructures. We are also aware of transfers taking place via illicit money transfer services or legitimate international money transfers before the funds are introduced into the illegal economy.

Cryptoassets

Due to the complexity and rapid global reach of cryptoassets, PST is seeing increasing use of these assets by extremists to send and obtain funds intended for terrorist financing. Some cryptoassets also offer varying degrees of anonymity, making the financial flows difficult to trace.

For more than a decade, Islamist extremists have been experimenting with various types of cryptocurrencies, and some IS affiliates have used their propaganda channels to encourage supporters to donate to their activities using cryptocurrencies such as Bitcoin[35] and Monero.[36]

Since 2022, the use of cryptocurrencies, FinTech companies[37] and other digital payment methods has increased markedly among Islamist extremists. Groups with a more regional focus, such as Hamas, have also been quick to adopt cryptocurrencies. For several years, Hamas has asked for donations to be made in cryptocurrency and has established several cryptocurrency exchange offices in or

---

[34] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[35] Bitcoin is a decentralised digital currency launched in 2009 that operates without central banks or intermediaries.

[36] Monero (XMR) is a decentralised, open-source cryptocurrency with a strong focus on privacy, anonymity and untraceability. Unlike Bitcoin, Monero automatically conceals the sender, recipient and transaction amount in all transactions, using advanced technology.

[37] FinTech (financial technology) is an umbrella term for technology used in financial products and services, which can include payments, savings, financing, stock trading and insurance.

near its areas of operation. This makes it easy for them to convert cryptocurrency into cash, which is essential for making use of the donations on a large scale.[38]

Cryptocurrency has also become a key component of IS's overarching financing strategy, and donations to ISKP's[39] media unit in Bitcoin, Ethereum[40] and USDT[41] have been reported, apparently in response to active propaganda and recruitment campaigns. One specific example is a recruitment operation in Tajikistan, in which ISKP raised USD 2 million in USDT from global sympathisers. Once converted into cash, ISKP can use couriers to distribute the funds as needed, pay for goods and services, or cover other expenses, such as wages.[42]

Identified transaction flows often involve different cryptoassets, multiple blockchains,[43] shared crypto addresses,[44] wallet providers[45] and cash-out mechanisms. These transaction flows can be difficult to trace because the various methods involved can obscure both the sender and the ultimate recipient.

It is difficult to quantify the scope of cryptocurrency exploitation aimed at terrorist financing in and from Norway. Greater accessibility, wider acceptance among terrorist organisations and the development of increasingly specialised products designed to strengthen anonymity make it extremely difficult to identify and disrupt terrorist financing transactions in cryptocurrency. Nevertheless, PST is seeing a general increase in the use of cryptocurrency by terrorist groups and lone actors, including in combination with other methods.

Cryptocurrency has been used in terrorist attacks in the West in an attempt to conceal the financial flows. There are also several cases in which Islamist extremists in the

---

[38] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[39] ISKP (Islamic State Khorasan Province) is part of the so-called Islamic State and is primarily based in Afghanistan.

[40] Ethereum is a decentralised, open blockchain platform best known for enabling smart contracts and decentralised apps (dapps). Unlike Bitcoin, Ethereum is a programmable platform that acts as the 'fuel' for network transactions.

[41] USDT, or 'Tether', is a stablecoin; a type of cryptocurrency designed to maintain a stable value that closely tracks the US dollar. It serves as a bridge between traditional currencies and the crypto market and is widely used to preserve the value of funds, trade cryptocurrencies without major price fluctuations, and make rapid transfers.

[42] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[43] A blockchain is a decentralised, distributed digital ledger that enables digital transactions to be recorded, tracked and verified. A blockchain stores data in blocks that are linked to one another using cryptography. The best-known application of blockchain technology is cryptocurrencies such as Bitcoin.

[44] A crypto address is a unique identifier consisting of a sequence of letters and numbers, used to send and receive cryptocurrency, similar to a bank account number.

[45] A crypto wallet is a digital tool that allows users to store, send and receive cryptocurrency. It serves as an interface between the user and the blockchain, where the user's digital assets are stored.

Nordic countries have used cryptocurrency in connection with illicit money transfer services and terrorist financing. Extremists have been found to use cryptocurrency to transfer funds to various fundraising activities promoted in IS propaganda, with the aim of supporting IS operatives and their families held in camps in northern Syria and Iraq.

Prepaid cards

The purchase of prepaid cards loaded with a fixed amount of electronic money has been identified as an alternative to transfers through traditional bank accounts, credit cards and cash. These payment cards are easy to transport and can be used to make transactions through a wide range of service providers, such as Visa and Mastercard. So-called 'open-loop'[46] cards appear to be more attractive because they can easily be used in shops and Automatic Teller Machines (ATMs) worldwide.[47]

Refer also to Økokrim's discussion of gift cards in the 2026 NRA.

Gold and luxury goods

Trade in luxury goods, including cars and artwork, can also be used to finance terrorism. The same applies to trading in commodities such as gold and diamonds. These goods are physical stores of value that are easy to transport and sell abroad. They can be used directly or exchanged for other goods needed to sustain terrorist activities.

Gold is a globally accepted high-value commodity that is difficult to trace. In Norway, gold can be traded relatively anonymously and is easy to smuggle across borders. PST is aware that gold is extensively bought and sold in Norway and transported across national borders.

Reference is also made to the chapter 'Non-monetary assets: physical and digital valuables' in Økokrim's NRA, as well as its discussion on indicators of concealed financial flows.[48]

[46] 'Open-loop' cards are prepaid cards that can be used in the same way as ordinary bank cards.

[47] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[48] Økokrim, National Risk Assessment, 2026

6 Selected obliged entities at particular risk of exploitation for terrorist financing

Banks, payment services and providers of cryptoasset services are particularly vulnerable to exploitation for terrorist financing. Traditional banking services continue to be used to place, hold and transfer funds, often through the use of frontmen, family members, 'neobanks' or virtual IBANs, which can help conceal the true purpose of transactions and the identity of recipients. New payment services and cross-border payment intermediaries create additional opportunities for terrorist financing. Cryptoasset service providers are considered particularly vulnerable to exploitation for terrorist financing as they serve as an entry and exit point to the conventional financial system.

Taking the indicators, methods and assets described above into account, PST considers banks, payment services and providers of cryptoasset services to be at particular risk of exploitation by individuals seeking to finance terrorism. It should be noted that other obliged entities besides those mentioned here could also potentially be exploited for this purpose. All obliged entities are expected to independently assess the terrorist financing risks associated with their activities and exposure.

Banks

Based on the data available to PST, there are indications that financial services offered by banks continue to be exploited for terrorist financing. This is despite the increased focus on measures to regulate the sector in relation to, for example, the identification of beneficial owners, transparency, identity verification and supervision.

Internationally, banks are considered to be at a high risk of exploitation for terrorist financing. Global reports indicate that traditional bank accounts continue to be used by transnational terrorist groups to place and store funds. This can involve the use of frontmen or intermediaries, front companies, as well as the establishment of companies and bank accounts across multiple jurisdictions to conceal identities etc. Traditional bank accounts are also used more frequently in areas under the control of terrorist organisations.[49]

[49] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

PST has observed that so-called neobanks[50] based abroad and operating across borders are involved in an increasing number of cases where there are also indications of, or suspicions of, terrorist financing. Regulatory compliance is often weaker in these institutions, or they may operate from countries where regulation and oversight are less stringent.

Virtual IBANs (vIBANs) have attracted increasing attention during the reporting period. A vIBAN is a digital bank account number that is not directly linked to a physical bank account, but instead functions as an alias or sub-account of a main account. VIBANs represent a terrorist financing risk because they can be used to conceal the origin of funds and make it more difficult for obliged entities to carry out their checks. PST has observed the growing use of vIBANs in attempts to finance terrorism, which is something obliged entities should be particularly alert to.

Through international cooperation, it is reported that funds stemming from both unsecured and secured credit[51] continue to be used to finance terrorism, including foreign terrorist fighters and local attacks. In many cases, the funds are obtained by falsifying documents or with the assistance of close family members to conceal the ultimate recipient. PST has found that known Norwegian extremists often use family members' accounts or accounts linked to terrorist organisations when transferring money to other known extremists.

Transactions by extremists and transfers for terrorism-related purposes are often for relatively small amounts. This makes them difficult to detect, particularly when methods such as those described above are used.

For further information, refer to Økokrim's description of the relevant risks to the banking sector in its NRA of money laundering.

Payment services

The number of new payment services has increased in recent years. Many of these offer money transfer and payment services both in person and online. Many operate as intermediaries in payment chains, making transaction flows more complex as funds pass through multiple stages, including across borders, before reaching the ultimate recipient. The sector is also characterised by innovation, which enables funds to be moved more rapidly across national borders. Many payment service

[50] In this context, the term refers to banks operating exclusively online.

[51] For example consumer loans and mortgages etc.

providers also offer their services from abroad, including from jurisdictions with less transparency or oversight.

PST's data indicate that payment services are increasingly being used to move money rapidly across borders as a means of obscuring transaction flows. PST has observed active use of electronic money transfer services[52] by Norwegian extremists. These services facilitate transactions between extremists in Norway and, perhaps especially, transfers out of the country for onward forwarding for terrorist activity. We are seeing differences in regulation and compliance across jurisdictions increasingly being exploited to conceal the ultimate recipient and sender of funds.

PST sees a particular risk associated with agents of foreign payment institutions, which can carry out payment intermediary services for Norwegian customers on the basis of a licence issued in another EEA country. These agents process transactions quickly and primarily handle small, cross-border payments, often to high-risk areas. Norway's Anti-Money Laundering Act is only partly applicable to these agents, which limits the scope for national oversight. This makes the method attractive to terrorist actors, as the speed of transactions, lack of safeguards and inconsistent oversight can help conceal the intended purpose and destination of funds.

Many of the transactions carried out in this sector can also be regarded as one-off transactions where no customer relationship is established, meaning that fewer customer due diligence requirements apply under the regulatory framework. The services appear to be increasingly used by vulnerable or higher-risk individuals, including people on the margins of society who have limited access to traditional banking services for making transfers abroad. The services are also highly susceptible to abuse by criminals exploiting existing weaknesses in regulation, procedures and controls. This has made the sector more vulnerable to terrorist financing.

For further information, refer to Økokrim's description of relevant risks in the sector in its NRA of money laundering. Many of the characteristics that make the sector vulnerable to money laundering also make it attractive to actors seeking to finance terrorism.

[52] Examples of digital money transfer service providers include PayPal, Wise and Revolut. It should be noted that Revolut and PayPal are also licensed as banks.

Cryptoasset service providers

Cryptoassets are becoming an increasingly attractive means of financing terrorism as they facilitate rapid, high-value transactions across jurisdictions. Cryptoasset services are considered particularly vulnerable to exploitation for terrorist financing as they serve as an entry and exit point to the conventional financial system. Although cryptoassets facilitate the movement and concealment of funds, fiat currencies[53] remain the primary target for terrorist actors because of their tradability and market value. Cryptoasset services are therefore a critical point of control for preventing terrorist financing.

PST's data indicate that cryptoassets are often used to move assets out of Norway. We have observed transfers from Norway to foreign actors, for example in jurisdictions with less stringent controls, or to actors that permit trading in cryptoassets that are anonymous or less traceable. These funds have subsequently been transferred to addresses associated with terrorist organisations. PST has nevertheless found it challenging to determine the extent to which funds have been transferred with the intention of financing terrorism.

For further information, refer to the discussion of cryptoassets in the NRA's section on money laundering, including the potential for exploitation of national cryptoasset service providers, particularly where foreign actors are involved.[54]

[53] 'Fiat currency' refers to currency issued by a government authority, typically a central bank, that is recognised as legal tender in a specified jurisdiction. Examples include Norwegian kroner, US dollars and euros.

[54] Økokrim, National Risk Assessment, 2026

7 Illegal and unregulated activities

Illegal and unregulated activities create a major opportunity for terrorist financing. Illicit payment intermediary services provide international channels for forwarding financial contributions and are often associated with criminal actors. Criminal actors also seek to exploit professional enablers to conceal their activities, both through the use of professional intermediaries and through direct assistance from, for example, lawyers and accountants.

Opportunities for fundraising have increased considerably in line with technological advancements, and terrorist actors can exploit the geopolitical situation to disguise terrorist financing as humanitarian aid.

Other technological advancements, such as digital platforms, provide further opportunities for covert transactions with little or no traceability, which international terrorist organisations are increasingly exploiting. Alternative assets such as gold and gambling activities continue to be popular means of transferring funds intended for terrorism due to their high value and limited traceability.

Illicit payment intermediary services

According to international reports, illicit payment intermediary services, including illicit money transfer services, are widely used to move funds intended to support terrorist activities. Extremists, for example, use their own networks to receive and transfer funds across borders and to store assets on behalf of the group. These networks, such as ISKP in Afghanistan, are integrated into other IS-related financial structures that support IS's global financial operations.[55]

It is also reported that almost all terrorist groups can be linked to the use of illicit or unregulated payment services. These are also used internally to transfer funds within the organisation, pay foreign terrorist fighters and cover costs associated with recruitment, travel, accommodation and operational activities. The same applies to financial contributions from diaspora communities, which are often channelled to terrorist organisations in other countries through such illicit money transfers.[56]

[55] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[56] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

Illegal services are also used to conceal proceeds from criminal activity involving cross-border transactions, such as drug trafficking and smuggling. PST has also seen indications that funds transferred as part of other criminal activity using such networks can ultimately have contributed to both intended and unintended terrorist financing. This is described in more detail in the section on ‘Links to criminal networks’ in Chapter 4.

PST has data supporting the finding that funds are transferred out of Norway through individuals and businesses offering illicit money transfer services in the market. However, the intermingling of funds makes it difficult to determine how much of the money is transferred to finance terrorism. The risk is heightened by the broad scope for misuse and the ease of access to such services.

Professional enablers

Økokrim defines professional enablers and insiders as, for example, accountants, bank advisers and lawyers who can facilitate money laundering and/or terrorist financing. They do this by assisting with the opening of bank accounts, providing client accounts, concealing beneficial owners and financial flows, arranging loans, or ‘turning a blind eye’ in key gatekeeper roles.[57]

Extremists may use professional enablers to transfer and conceal the traceability of funds intended for terrorist financing. Despite the seemingly high demand for these enablers, it is PST’s assessment that they tend to be used more for money laundering than for terrorist financing.

Extremists’ transactions are typically for small amounts, and the total amounts involved are rarely substantial compared with those seen in money laundering. Nevertheless, we have observed that some degree of facilitation can be necessary to channel funds to the intended recipients. For example, terrorist organisations such as al-Qaeda and IS have needed intermediaries to act as links between donors and operational groups.[58] Consequently, there is a risk that such intermediaries may also exist in Norway. Obliged entities should therefore have a special focus on identifying professional enablers.

There may also be cases in which extremists actively seek to mislead professional enablers. Obliged entities often find it challenging to identify suspicious transactions because of their large customer base and high workload. Accountants, who are more

[57] Økokrim, National Risk Assessment, 2026

[58] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

directly involved in processing clients' accounting records, are considered to be more exposed to risk than auditors, who review the material retrospectively. The data show that the number of reports of suspected terrorist financing submitted by lawyers has been low compared with the number submitted by accountants and auditors. This may indicate a need for greater expertise in terrorist financing within the sector in order to reduce the risk of exploitation.

From a terrorist financing perspective, the use of false invoices and receipts is also a potential risk, particularly in light of the ability of generative AI to fabricate receipts. Extremists may seek to include apparently legitimate invoices and receipts in accounting records in order to mislead accountants and auditors and thereby conceal terrorist financing activities.

To date, PST is not aware of any Norwegian extremists using professional enablers to any great extent. Nevertheless, opportunities exist, and there is therefore a risk that they could be used to support terrorist financing in and from Norway.

The general risk associated with professional enablers is described in further detail in Chapter 6 of Økokrim's NRA.[59]

Raising funds and other assets

Raising funds and other assets in Norway is not regulated by law. There is also no requirement to register such activity or notify the authorities. Individuals and closed groups can therefore carry out fundraising activities without having to establish an organisation.

PST has observed that Norwegian extremists sometimes organise fundraising activities themselves, but it is more common for them to take part in fundraising organised by others. The purpose of their fundraising is often unclear. For example, Islamist extremists use religious settings, such as mosques, to collect money through zakat[60] and similar means. This method is suitable for generating large sums by exploiting donors' religious convictions, and there is a risk that the funds raised may be used to finance terrorism. Several cases have been identified in which funds have been raised from Norwegian donors for terrorist purposes.

We have also seen instances of individuals who are not affiliated with a charitable organisation launching fundraising campaigns under the guise of humanitarian or

[59] Økokrim, National Risk Assessment, 2026

[60] The term 'zakat', meaning 'almsgiving', is one of the five pillars of Islam. The others are shahada (faith), salah (prayer), sawm (fasting during Ramadan) and hajj (pilgrimage).

social causes, where the funds raised may ultimately be used to support terrorist activities or extremists. Humanitarian and charitable causes can serve as effective 'fronts' and are therefore vulnerable to exploitation for terrorist financing. Examples of charitable causes that are open to exploitation include the conflicts in Gaza, Syria and the Horn of Africa.[61]

In recent years, new technology has enabled more effective fundraising. PST is aware of individuals and organisations in Norway that have initiated fundraising campaigns for foreign terrorist fighters with links to Norway and international terrorist organisations, without being registered with, for example, Charity Monitoring Norway.[62]

A trend has been observed among Norwegian Islamist extremists whereby funds are raised to support or facilitate the escape of IS-affiliated foreign terrorist fighters and their families from camps and prisons in Syria. Several networks have raised funds that have subsequently been transferred via illicit money transfer services to, for example, the al-Hol[63] camp in Syria. Those responsible for the various fundraising campaigns accept various forms of payment, including cryptocurrency. In their social media channels, group chats and online profiles, the fundraisers state that the funds will be used to improve detainees' conditions or secure their release.[64]

Engaging in fundraising to finance terrorism-related activities abroad is less common among Norwegian right-wing extremists. Historically, fundraising has instead tended to be used primarily to provide personal support for other right-wing extremists. For example, within the more hierarchical groups in the Nordic countries, money has been raised to provide financial support for members who have served prison sentences, or to support members in other ways as needed.

PST's data indicate that the risk of fundraising to support terrorist financing is partly shaped by the broader geopolitical situation, with a heightened risk during periods of geopolitical uncertainty and humanitarian crises.

---

[61] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[62] Charity Monitoring Norway is a Norwegian foundation that works to ensure that fundraising activities are carried out responsibly.

[63] Al-Hol is a refugee camp in Syria housing a large number of women from areas formerly controlled by IS.

[64] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

Social media, digital platforms and gift cards

'In national and transnational online networks on encrypted platforms, users can operate and communicate anonymously, while building the relationships and trust necessary for terrorist planning and support activities.'

- National Threat Assessment 2026 (PST)

PST has observed that various digital platforms are widely used as supplementary tools to obscure or conceal money transfers.

Online fundraising campaigns are typically advertised openly on social media but may also be disguised as appeals for humanitarian relief or other charitable causes. Increased use of QR codes has been documented among various terrorist groups to solicit donations or share cryptocurrency wallet addresses. Encrypted communication apps are also widely used because they enable secure discussions about payment methods and the real intended use of the funds.[65]

Use of encrypted messaging applications such as WhatsApp, Telegram, Viber, Signal etc. by terrorist organisations and lone actors is on the increase. These platforms offer private conversations that protect users' anonymity. Extremists use these services to share financial information (e.g. IBAN numbers, cryptocurrency wallet addresses or other payment details) and to securely provide instructions for making donations. Features such as 'self-destructing' messages, which are automatically deleted after a predefined period, make it more difficult to trace such communications.[66]

The facilitation of covert transactions through messaging services can pose significant challenges in terms of traceability. Once funds enter the payment system, the information available about the ultimate recipient is extremely limited. Only by cross-referencing this information with data held by the relevant social media platform is it possible to establish the true purpose of the transactions. For outgoing transfers from the internal platform, the transaction information may reveal something about the original social media platform, but in many cases it will only identify financial intermediaries, making it difficult to establish the source of the funds.[67]

As such tools become more popular, accessible and profitable, terrorist organisations and lone actors are increasingly finding ways to use them to raise funds. Some

[65] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[66] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[67] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

terrorist groups have reportedly used TikTok fundraising campaigns, exploiting features such as filters and games to generate funds. In Sweden, a 24-year-old man was imprisoned for terrorist financing offences after raising approximately SEK 500,000 through TikTok between July 2022 and July 2023, which he then transferred to individuals linked to IS.[68]

It is important to note that there is also considerable scope in Norway to support such initiatives organised from abroad. This is because it is difficult to obtain information about the integrated payment functions offered by the various social media platforms.

PST is aware that extremists have started using e-commerce platforms[69] to purchase equipment, weapons, chemicals and 3D-printing materials for operational purposes. This is more discreet than making purchases in person. These platforms can also be used to sell goods to finance terrorist activities and to transfer funds in ways that resemble trade-based money laundering. Traded goods can thereby serve as a cover for assets transferred between members of a network.

Gold dealers

Gold is a universal currency that can be used worldwide. It is particularly attractive in countries with poorly functioning financial systems.

At present, Norwegian dealers in gold products are not required to submit reports of suspicious transactions to Økokrim's Financial Intelligence Unit (FIU). However, there are several indications that gold dealers are being exploited as part of terrorist financing activities. PST is aware of significant activity in the sector and that several extremists, both in Norway and abroad, can be linked to extensive gold trading.

Gambling and gaming

Illegal gambling

Illegal and unregulated gambling has been identified as a significant and growing terrorist financing risk globally, including by FATF.[70] The financing of terrorism can be facilitated through the generation of income, match-fixing, the use of frontmen and

[68] Suspected of financing terrorist group via TikTok and cryptocurrency – 24-year-old convicted, SVT News

[69] An e-commerce platform is a software application that enables businesses and private individuals to sell products and services online.

[70] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

intermediaries, combinations of illegal gambling and cryptoassets, opaque payout structures, etc.

As noted in the NRA of money laundering, the Norwegian Gambling and Foundation Authority estimates that the unregulated gambling market in Norway was worth between NOK 1.7 and 2.0 billion in 2025.[71] Foreign gambling services are not subject to the same loss and stake limits as Norwegian gambling companies and are therefore more attractive for money laundering as well as terrorist financing. There is a large market for foreign online gambling, including casinos, poker and sports betting. These operators are not permitted to offer gambling services in Norway, but are nevertheless accessible to and targeted at Norwegian citizens. It is also unclear who is actually behind many of these gambling services.

Transactions through foreign gambling platforms have also been used as a cover. Transfers to gambling accounts appear to be intended for gambling, but in reality the funds are transferred from the account to the intended recipient without being used for gambling at all.

Pyramid and Ponzi schemes[72] are at increased risk of being misused for terrorist financing. PST has observed that terrorist groups have used Ponzi schemes to generate funds that, either directly or indirectly, are used to support terrorist activities. The funds are often laundered to conceal their true destination.

Interpol has reported a transnational case involving 17 countries worldwide. The case originated from a cryptocurrency-based Ponzi scheme. The operation had more than 100,000 victims and resulted in estimated losses of more than USD 500 million. Interpol's investigation found that several of the cryptocurrency wallets used may potentially be linked to terrorist financing.[73]

It is unclear whether terrorism has been financed in or from Norway using this method. Given the scale of the illicit activity, as well as the potential unreported figures, PST assesses that it cannot be ruled out that such funds have been channelled to terrorist financing, particularly abroad.

---

[71] Norwegian Gambling and Foundation Authority, Responsible Gambling and Channeling at Norsk Tipping and Norsk Rikstoto, March 2026. Net turnover is stakes minus winnings paid to players, 2026.

[72] A Ponzi scam (or Ponzi scheme) is a form of investment fraud in which returns are paid to previous investors using money from new investors, rather than from genuine profits.

[73] Interpol, 83 arrests in landmark African operation against terrorism financing, 2025

Online gaming and in-game items

We have observed that some terrorist groups, including right-wing extremist groups and Hezbollah, develop and sell their own video games both as propaganda tools and as a source of funding. These games are available on the open internet. There is also documented use of transactions involving 'in-game items' by some right-wing extremist groups. These in-game items can be purchased and donated to other players with little traceability.[74]

PST does not have specific data on whether gaming platforms are being used for terrorist financing in Norway. However, it is aware that several Norwegian banks have seen an increase in the number of customers transferring small or medium-sized amounts to such platforms. Large transfers are also reported from time to time, and there are examples of boys and young men making large monthly transfers to gaming platforms.[75] So far, however, we have not been able to establish any link between these transactions and terrorist financing. Nevertheless, the trend and scale of the activity indicate an increased risk of funds being concealed through online gaming. We refer here to the discussion above on the radicalisation of minors.

There is a risk that the increasing use of video games could be exploited to encourage children and young adults to become involved in financing terrorism-related activities.

8 Vulnerability landscape

Uncovering terrorist financing is complicated. An increasing number of actors are involved in transaction flows spanning national borders and jurisdictions. This increases the opportunities for concealing the senders as well as the recipients of funds.

Cross-border transaction flows involving multiple actors also make it difficult to trace funds, and even more difficult to determine that funds have been transferred for the specific purpose of supporting terrorist activity. Individual contributions are often relatively small, and when transferred through legitimate channels, it becomes even more challenging to distinguish them from other, lawful financial flows.

[74] FATF, Comprehensive Update on Terrorist Financing Risks, 2025

[75] Økokrim, Financial Intelligence Unit Annual Report, 2025

The increasing convergence of conventional and digital methods of fundraising and transferring funds further complicates the picture.

The complexity of today's financial/transaction flows require both a sound understanding of the phenomenon and access to multiple sources of information in order to determine whether a particular case involves terrorist financing. This presents challenges in the efforts to prevent and investigate terrorist financing. The difficulty lies in whether the transaction can be traced and deciding if it was carried out with the intention of financing terrorism.

Available methods and capacity

During the reference period, PST has observed that an increasing proportion of transfers linked to terrorist financing are shifting away from regulated services and into the illegal and unregulated market.[76] This includes, but is not limited to, peer-to-peer (P2P) transactions and transactions facilitated by individuals and networks that provide payment intermediary services outside the legal economy. This shift is also increasingly facilitated by complementary technologies, such as encrypted messaging services used in combination with AI, and cryptoassets on different blockchains.

Given the current regulatory framework, division of responsibilities and allocation of powers in the prevention of terrorist financing, this shift requires greater cooperation between all relevant actors, including obliged entities, to identify and prevent terrorist financing activity and prosecute those responsible.

Insufficient analytical and investigative capacity among the relevant authorities therefore represents a vulnerability, as it limits their ability to identify indicators of terrorist financing and take preventive action and pursue criminal proceedings.

Few cases in Norway have resulted in convictions for terrorist financing. It is nevertheless important to note that financial trails, analysis of transaction flows and information on financial activity are important sources of information for PST, including in cases that do not explicitly concern terrorist financing.

Other vulnerabilities of the Norwegian framework

Despite an increase in the number of suspicious transaction reports, there continue to be shortcomings in compliance with the applicable regulatory framework. Several

[76] Despite the observed shift towards illegal and unregulated activities, funds intended to finance terrorism continue to be transferred through the exploitation of regulated services.

evaluations of Norway's efforts to counter terrorist financing have identified various shortcomings that impact on the effectiveness of Norway's supervisory framework.[77]

One vulnerability relates to the generally limited understanding of terrorist financing in Norway. Recognising relevant methods and identifying the potential actors behind them is challenging, which limits the data available for further analysis. A key vulnerability is the data available for assessing whether opportunities for terrorist financing are actually being exploited nationally. Meanwhile, there is generally limited systematic sharing of data between public authorities on trends in terrorist financing, its scale and the effectiveness of measures taken to address it. The existing knowledge base is largely sourced from general threat assessments, descriptions of methods observed internationally and individual cases.

This means that more is currently known about potential vulnerabilities and possible methods of terrorist financing than of trends, scale and the effectiveness of measures taken to address it. Consequently, many of the findings should not necessarily be interpreted to mean than terrorist financing does not take place.

As noted in the NRA of money laundering, many public authorities involved in efforts to counter terrorist financing also operate in silos, with a strong focus on the boundaries of their respective mandates. This, in turn, hampers information sharing not only between different authorities, but also with the private sector and other actors contributing to the overall effort to counter terrorist financing. A lack of focus on vulnerabilities also presents a challenge to the national implementation of an effective resilience framework.

Furthermore, authorities and obliged entities often take a long time to develop the necessary expertise, tools, supervisory arrangements and regulatory frameworks commensurate with the actual risk. This also applies to rules governing information sharing and systems that enable the rapid and effective exchange of information, including across national borders. As a result, extremists can adopt new digital tools faster than authorities and platforms are able to adapt, allowing them to operate unhindered.

We also refer to the vulnerabilities described in the NRA's section on money laundering, several of which are also relevant to the efforts to counter terrorist financing.

[77] See, for example, FATF's follow-up report on its evaluation of Norway (2023) and the IMF's report on anti-money laundering efforts in the Nordic and Baltic countries (2023).

State actors

'We expect Iranian intelligence and security services to conduct intelligence and influence operations in Norway in 2026. The Iranian regime may also attempt to target Western interests through damage to property, targeted assassinations, terrorist acts or destructive cyber operations.'

- National Threat Assessment 2026 (PST)

PST's data indicate that some foreign terrorist organisations have received, and continue to receive, financial and other support from state actors. State support for terrorism can take several forms, including direct financial support, logistical and material support, and training. State support combined with sanctions evasion techniques involving trade or the smuggling of raw materials makes it more difficult for obliged entities and security services to uncover potential terrorist financing.

Obliged entities in Norway should be alert to this type of financing. The risk is often indirect and concealed through geographical exposure, the use of intermediaries, complex ownership structures and cross-border transactions. This underscores the need for enhanced customer due diligence, a good understanding of beneficial ownership and an increased focus on whether seemingly ordinary customer relationships or payment flows may be part of the wider terrorist financing picture.

9 Consequences

Terrorist financing has consequences within Norway and beyond. In Norway, terrorist financing can help sustain and strengthen extremist networks, facilitate recruitment, propaganda and logistics, and in the worst case, enable the planning or execution of terrorist attacks. The consequences therefore extend beyond financial crime in the narrow sense: terrorist financing can increase the capacity of actors that pose a threat to life and health, national security and the public's sense of safety.

The transfer of funds from Norway to other countries for the purpose of financing terrorism can also have serious consequences, even when the associated act of violence takes place in another country. Such funds can help sustain terrorist groups, finance attacks, prolong conflicts and undermine international security. For Norway, this also entails a risk that the country could be used as a platform or intermediary in

international financing chains, which will have implications for Norway's security responsibilities and international obligations.

10 Overall risk assessment

The overall risk of terrorist financing is assessed as MODERATE. The actual scale appears to be limited, but the vulnerabilities and opportunities for exploitation indicate that the risk cannot be considered LOW. The risk of terrorist financing within Norway is assessed as lower than the risk of financing from Norway to other countries.

The assessment of the risk level is partly based on the fact that Norwegian extremists' international contributions to terrorist financing are generally considered limited, both in scale and number. In this context, PST has also observed that Norwegian actors lack the capacity to raise large sums, and that financing from Norway for terrorist activity abroad is rarely substantial. Although some contributions may be significant for lone actors or groups planning or carrying out specific attacks, these activities pose a relatively low risk in the global context. Norway's role as a source of funding for international terrorism therefore remains marginal, although funds from Norway may still be significant for specific actors or operations.

The situation in Norway is similar. Terrorist financing is primarily channelled through individual actors, with contributions often being small and linked to their personal finances. Financing by Norwegian extremists within Norway is rarely directed towards large, organised terrorist networks, and the risk is mainly limited to supporting lone actors planning acts of violence in Norway. This may make it less challenging for Norwegian security authorities and obliged entities to prevent and monitor the activities of lone actors, but the phenomenon nevertheless presents clear security challenges.

Appendix

Section 135. Terrorist financing

A penalty of imprisonment for a term not exceeding 10 years shall be applied to any person who illegally provides, receives, sends, procures or raises money or other assets with the intent or knowledge that the resources will be wholly or partly used

a. to commit an act specified in section 131, section 134, 136 b or sections 137 to 144,
b. by a person or group whose purpose is the commission of acts specified in section 131, section 134, 136 b or sections 137 to 144, when the person or group has taken steps to achieve the purpose by unlawful means,
c. by an enterprise owned or controlled by someone specified in b), or
d. by an enterprise or a person acting on behalf or on the instructions of someone specified in b).

The same penalty applies to any person who makes banking or other financial services available to persons or enterprises specified in the first paragraph, b), c) or d).

Section 136 a. Penalty for participation, etc. in a terrorist organisation

A penalty of imprisonment for a term not exceeding 6 years shall be applied to any person who forms, participates in, recruits members into or provides financial or other material support for a terrorist organisation, when the organisation has taken steps to achieve the purpose by unlawful means.

Aiding and abetting is not punishable.



POLITIETS
SIKKERHETSTJENESTE

pst.no