COUNCIL OF EUROPE'S COMMITTEE OF EXPERTS ON THE
EVALUATION OF ANTI-MONEY LAUNDERING MEASURES
AND THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2025)27

Money Laundering, Terrorism Financing and Proliferation Financing Risks and Trends Linked to Proceeds Obtained from Conflicts

Typologies report

December 2025

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The Typologies Report on Money Laundering, Terrorism Financing and Proliferation Financing Risks and Trends Linked to Proceeds Obtained from Conflicts was adopted by the MONEYVAL Committee at its 70th Plenary Session (Strasbourg, December 2025).

Table of Contents

Abbreviations and acronyms 4

Executive Summary 5

Introduction 6

Key Findings 7

Topical Sections 8

1. Proceeds and conflict – ML/FT/PF risks and threats in national risk assessments 8

    1.1. Proceeds and conflict 8

    1.2. ML, TF and PF risks and threats related to conflicts and NRAs 10

    1.3. Conclusion 11

2. Laundering of proceeds from conflict and/or their use for TF/PF – key emerging trends 12

    2.1. Different methods, actors and typologies used for the laundering of proceeds from conflict and/or their use for TF/PF 12

    2.2. Conclusion 22

3. Risk mitigation measures 23

    3.1. Overview of global and regional AML/CFT/CPF measures in the context of armed conflict 23

    3.2. Examples of sanctions relating to illegal financial proceeds from conflict 25

    3.3. The practice of blocking, suspending, or freezing conflict-related transactions and assets 26

    3.4. Application of confiscation to conflict-related assets of sanctioned persons 27

    3.5. Case law in the area of conflict-related sanctions policy 28

    3.6. Strategic documents 28

    3.7. Conclusion 29

Abbreviations and acronyms

AML	Anti-money laundering
CFT	Countering the financing of terrorism
CPF	Counter-proliferation financing
Egmont	Egmont Group of Financial Intelligence Units
EU	European Union
FATF	Financial Action Task Force
FIU	Financial intelligence unit
ML	Money laundering
MONEYVAL	Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
NGO	Non-governmental organisation
NRA	National risk assessment
PF	Proliferation financing
TF	Terrorist financing
TFS	Targeted financial sanctions
UN	United Nations
UNSC	United Nations Security Council
VAs	Virtual assets
VASP	Virtual asset service provider

Executive Summary

Contemporary conflict dynamics extend beyond conventional military confrontations and encompass hybrid strategies, such as cyber-attacks, disinformation, and economic coercion, creating an increasingly permissive environment for financial crimes. These conditions weaken governance structures, disrupt regulatory oversight, and create space for illicit financial flows, including money laundering (ML), terrorist financing (TF) and proliferation financing (PF).

The objective of this Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) typology research examines how conflicts create conditions for obtaining the illicit proceeds, how they are laundered and/or used for TF/PF. The project aims to identify the relevant patterns, trends and vulnerabilities to strengthen anti-money laundering (AML), combating financing of terrorism and proliferation financing (CFT and CPF) frameworks and international co-operation.

The analysis underlines that, due to weakened state control and destabilised markets, conflict zones often become incubators for complex, interconnected criminal economies where illicit proceeds are generated, laundered, and reinvested to perpetuate violence and destabilisation. The analysis emphasises the growing sophistication of illicit financial mechanisms used to circumvent targeted financial sanctions (TFS), particularly in the context of PF. Conflict-affected environments enable criminals to exploit vulnerabilities in financial and regulatory systems, making use of complex schemes involving shell companies, third-country intermediaries, and virtual assets (VAs) to conceal the origin, movement and purpose of funds.

While some jurisdictions have begun to recognise these risks in their national risk assessments (NRAs), most have yet to fully integrate conflict-related threats into their AML/CFT frameworks. Strengthening cross-border co-operation, enhancing public-private information sharing, and engaging with actors active in conflict-affected areas, such as non-governmental organisations (NGOs) and international organisations, are key steps to address the complex and evolving ML, TF and PF risks associated with proceeds obtained from conflicts. Importantly, even jurisdictions not directly affected by conflicts may become conduits or facilitators of these illicit flows, underscoring the need for heightened vigilance and robust cross-border co-ordination within the global AML/CFT framework.

Tools such as the FATF Standards,[1] United Nations (UN) TFS[2] and European Union (EU) restrictive measures,[3] international co-operation through the Egmont Group, and regional enforcement mechanisms, play a central role in curbing illicit financial flows linked to conflicts. The effectiveness of these measures, however, depends on consistent implementation, strong legal frameworks, and co-ordinated action across public and private sectors. As the typologies and techniques used to launder proceeds from conflicts evolve, jurisdictions must enhance their detection and enforcement capacities and ensure that AML/CFT measures remain agile and responsive to the challenges posed by contemporary conflicts dynamics.

1. The FATF Recommendations (often referred to as the FATF Standards) provide a comprehensive framework of measures to help countries tackle illicit financial flows. See: FATF Recommendations, available at https://www.fatf-gafi.org/en/topics/fatf-recommendations.html.
2. Targeted Financial Sanctions (TFS) are restrictive measures imposed by the United Nations to maintain international peace and security, particularly in response to terrorism. See: Sanctions, available at https://main.un.org/securitycouncil/en/sanctions/information.
3. EU restrictive measures (often referred to as 'EU sanctions') are intended to bring about a change in bad or harmful policies or activities by targeting the non-EU countries, including organisations and individuals, responsible. See: Overview of sanctions and related resources, available at Overview of sanctions and related resources - Finance - European Commission.

Introduction

1. The primary aim of this analysis is to examine how illegal proceeds arise from regions affected by armed conflicts[4] and/or military aggression[5] (hereinafter 'conflict'), how these proceeds are laundered, used to finance terrorism and the proliferation of weapons of mass destruction, and how such risks may be mitigated through improved understanding and co-ordinated response. The analysis is intended to support MONEYVAL delegations by addressing a thematic area that is frequently underrepresented in national risk assessments (NRAs).

2. MONEYVAL's 2023 – 2027 Strategy,[6] adopted on 25 April 2023 in Warsaw, Development Objective 2.3, calls for *"developing a research-based understanding of major ML/TF trends and underlying rule of law and economic factors."* As acknowledged in the Strategy, AML/CFT intersects with broader issues of economic governance, rule of law, and human rights. Although significant thematic research in this field is conducted by academic institutions, investigative journalists, NGOs, and private sector actors, MONEYVAL's operational typologies work provides an opportunity to advance institutional understanding of complex and emerging issues. Within this strategic context, MONEYVAL agreed to explore this thematic issue in greater depth through a targeted study on *proceeds obtained from conflict and/or military aggression*.

3. The project was conducted by a dedicated working group composed of experts from Ukraine (Project Lead), Jersey, Lithuania, and the Republic of Moldova, with support provided by the MONEYVAL Secretariat. These jurisdictions volunteered to contribute their experience and insights to strengthen the understanding of ML, TF and PF trends related to proceeds obtained from conflict. In addition, data was collected through a questionnaire circulated among MONEYVAL delegations, with responses received from 17 jurisdictions (data from 2021 to 2023). Additional information and case studies were also collected (data from 2024 to July 2025) and information drawn from publicly available reports.

4. The analysis is divided into three topical sections:

    1. **Proceeds and conflict – ML/TF/PF risks and threats in national risk assessments:** explores conflict-related dimensions that enable obtaining illicit proceeds and how countries have identified and assessed relevant ML/TF/PF risks and threats.
    2. **Laundering proceeds from conflict and/or their use for TF and PF:** examines the laundering of conflict-related proceeds and/or their use in TF and PF, including different schemes and trends for obfuscation and transnational movement of illicit funds.
    3. **Risk mitigation measures:** outlines existing responses to these challenges, including international standards, regional co-operation, and sanctions enforcement, while identifying gaps and emerging trends that may require further attention.

4. '*An armed conflict is said to exist when there is an armed confrontation between the armed forces of different States, or between governmental authorities and organised armed groups or between such groups within a State (non-international armed conflict). Other situations of violence, such as internal disturbances and tensions are not considered to be armed conflicts*'. Source: *International Committee of the Red Cross – ICRC*, available at www.europarl.europa.eu/RegData/etudes/ATAG/2023/757582/EPRS_ATA(2023)757582_EN.pdf.
5. UN General Assembly Resolution 3314 (XXIX), in 1974, defined aggression as "*the use of armed force by a State against the sovereignty, territorial integrity or political independence of another state*", available at www.un-documents.net/a29r3314.htm.
6. MONEYVAL Strategy on anti-money laundering, combating the financing of terrorism and proliferation financing (2023-2027), Development Objective 2.3, available at https://rm.coe.int/moneyvalstrategy2023-2027-en/1680ab0b06.

Key Findings

1. Conflict environments enable the generation of illicit proceeds

Conflict creates vulnerable environment that enables the generation, movement, and concealment of illicit proceeds.

2. Conflict-related proceeds are laundered through complex mechanisms

Conflict-related proceeds are laundered through complex, transnational networks that blend formal and informal financial channels. Strengthening resilience against conflict-related illicit finance requires the understanding of the typologies being used, as well as the integration of such knowledge, together with geopolitical risk analysis, into AML/CFT/CPF efforts and strategies.

3. There is an uneven risk understanding and mitigation of conflict-related risks

While MONEYVAL jurisdictions recognise conflict-related financial risks, these are not yet systematically reflected in NRAs or supervisory practices. The gaps between risk identification, interagency co-ordination, and sanctions enforcement reduce the overall effectiveness of AML/CFT/CPF frameworks.

4. Domestic and international co-operation is key to addressing conflict-related risks

Enhanced co-operation among Financial Intelligence Units (FIUs), supervisors, and the private sector, and better use of data and technology to trace cross-border financial flows are needed for successful AML/CFT/CPF efforts against conflict-related illicit finance.

5. Conflict-related risks are diverse

The typologies identified in this study include the laundering of proceeds obtained from conflicts and their use for TF and PF, including TFS circumvention, exploitation of non-profit organisations (NPOs), and the misuse of Virtual Assets and shell companies to obscure ownership and fund movement.

6. Addressing risks emanating from conflict is essential in ensuring stability

Addressing the financial dimensions of conflicts is essential not only for safeguarding financial integrity but also for preserving regional stability, preventing corruption and proliferation, and reinforcing the collective security framework on which MONEYVAL jurisdictions depend.

Topical Sections

1. Proceeds and conflict – ML/FT/PF risks and threats in national risk assessments

General

5. This section examines the different ways through which proceeds are obtained from conflict and how related ML, TF and PF risks and threats have been assessed by MONEYVAL jurisdictions.

6. According to the Institute for Economics and Peace's 2024 Global Peace Index report, 56 'active conflicts' are identified globally, and 92 countries are engaged in conflicts beyond their own borders.[7] Modern conflicts have evolved beyond conventional military confrontations; they incorporate hybrid tactics, including cyber warfare, and economic coercion, creating new vulnerabilities for financial crime and illicit financing ('*Hybrid Warfare*').[8] While '*Hybrid Warfare*' does not always meet the traditional definition of conflict, nonetheless, it significantly impacts the security and stability of states.

7. Information and case examples provided by MONEYVAL jurisdictions demonstrate that conditions created by conflict facilitate the proliferation of ML, TF, and PF globally, and that these patterns are affected by the intensity, scale, and duration of an armed conflict. Overall, based on the analysis of the responses received from MONEYVAL jurisdictions, distinct forms of illegal proceeds can be noted as arising due to the armed conflict-related instability. These are outlined below.

1.1. Proceeds and conflict

8. Conflict generates instable environments that facilitate the emergence and expansion of illicit economic activity. The weakening of state authority and regulatory systems and the disruption of law enforcement mechanisms in conflict zones create permissive conditions in which proceeds are generated through a variety of illegal means, and not necessarily through the direct actions of warfare. These proceeds represent a distinct category of criminal income that must be considered in AML, CFT and CPF.

9. MONEYVAL jurisdictions have noted following main categories:

- *Corruption:* Corruption is a both a driver and a product of conflict-affected environments. Corruption undermines institutional effectiveness and enables hostile actors to embed themselves in administrative or political systems creating favourable conditions for ML, TF and PF of proceeds obtained from conflict.
- *Hybrid Warfare:* Hybrid warfare, which blurs the line between conventional military tactics and covert economic or informational strategies, plays a central role in the generation of illicit proceeds in conflict settings. These actions create permissive circumstances in which illicit financial flows are generated and channelled.
- *Cyber-crime schemes*, often transnational in nature and difficult to trace, benefit from the legal and technical gaps created by conflict-environment. While cyber-attacks primarily aim to undermine national security and disrupt state functions, they also serve as mechanisms to extort and misappropriate funds to support conflict. Factors that characterise cybercrime threats relating to conflict include the use of hacking to collect national security information;

7. Institute for Economics and Peace 2024 Global Peace Index report, available at GPI-2024-web.pdf.
8. NATO Review - Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote, available at https://archives.nato.int/nato-review-hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote.

the targeting of critical infrastructure; the infiltration of state bodies by actors linked to hostile states; and the employment of hackers in third countries.

- *Arms Trafficking, Narcotics, And Human Exploitation:* Conflict zones may become breeding grounds for illegal markets. The collapse of security, oversight and law enforcement infrastructures has been noted to allow arms trafficking, narcotics, and human exploitation. These markets generate significant illicit proceeds which, in some examined cases, also flow through organised criminal networks operating with the tolerance or active involvement of hostile states. Such activities are not confined to the territories affected by conflict; they extend across borders, facilitated by demand for these markets in external jurisdictions and the weakening of regulatory controls.
- *Smuggling of cash:* In conflict environments where border controls have weakened or collapsed, the movement of goods and funds becomes a significant channel through which proceeds are generated and laundered. These include proceeds from coal exports, the smuggling of counterfeit currency, the use of cryptocurrencies, and the illicit sale of gold and other natural resources. Such flows are often facilitated by local complicity or through networks operating beyond the conflict zone.
- *Abuse of NGOs*: Abuse of NGOs in conflict zones has also been observed to facilitate illicit financing under the guise of humanitarian or religious missions. Volunteers or personnel may unknowingly serve as conduits for illegal financial flows. In some cases, NGOs with the explicit purpose of channelling illicit funds have been established.
- *Abuse of VAs/VASPs*: Several cases provided by MONEYVAL members include examples where VAs/VASPs are used to disguise the proceeds obtained from conflicts.

10. Below are case examples provided by MONEYVAL members.

Case box 1 – Examples how conflict environments facilitate obtaining illicit proceeds

Case 1: As reported by one MONEYVAL member country facing armed conflict, the jurisdiction's security services recorded thousands of cyberattacks aimed at disrupting government communications and administrative functions across state jurisdictions. Among other impacts, this weakens the state's ability to fight serious crimes that enable obtaining illicit proceeds.

Case 2: In another case, a group of individuals (in a conflict area) used malware to attack over a thousand targets across multiple countries, demanding ransom payments in VAs. The proceeds of these cybercrime operations were laundered using virtual asset service providers (VASPs) and electronic currency platforms, demonstrating the convergence between cybercrime and illicit financial flows in the context of armed conflict.

Case 3: The third example provided related to the investigation of complex financial transactions between companies, including cyclical transfers labelled as financial aid, payments for industrial goods, and the issuance of loans to entities suspected of holding unaccounted cash. These operations appear to have facilitated the conversion of non-cash assets into cash to support armed groups operating within the conflict zone.

1.2. ML, TF and PF risks and threats related to conflicts and NRAs

11. The responses received to the questionnaire from MONEYVAL jurisdictions indicate that, between 2021 and 2023, most members had not directly assessed the ML, TF and PF risks and threats associated with proceeds obtained from conflict. In the most recent national risk assessments (NRAs) of the responding 17 jurisdictions, seven did not explicitly consider such ML/TF/PF risks or threats, whereas five did consider those risks, but not all of them identified any specific risk related to conflict. Four jurisdictions were in the process of updating their NRAs at the time responses were collected.

12. For a more comprehensive analysis, the NRAs of other four MONEYVAL jurisdictions which had not completed the questionnaire, but whose NRAs are publicly available, were also analysed. All of them have been published since 2021. Three of these four also considered the risks associated with armed conflict within the framework of their NRAs.

13. The analysis conducted for this report shows that most jurisdictions do not distinguish the risks directly related to armed conflict in their NRAs.

14. The MONEYVAL jurisdictions that completed the questionnaire identified the following ML, TF and PF risks relating to conflicts:

a) Money Laundering

i. Sanctions evasion
ii. Use of Shell Companies and similar legal structures for ML
iii. Removal of cash and money from conflict zones
iv. Theft and illegal removal of goods and natural resources into third party countries
v. Uncontrolled movement of individuals across international borders
vi. Forging of identify documents
vii. ML through the use of VAs
viii. ML through trade in assets stolen in conflict zones
ix. Illegal removal of small arms and ammunition from conflict zones by individual criminals

b) Terrorist Financing

i. Financing through use of VAs
ii. Using NPOs and crowdfunding activities to raise funds for terrorist groups
iii. Financing of private military companies and foreign terrorist militants
iv. Financing of illegitimate separatist, radical, and extremist organisations

c) Proliferation Financing

i. Co-operation between states subject to international sanctions regimes
ii. Improper or insufficient compliance with obligations regarding TFS

15. The jurisdictions that responded to the questionnaire for this report identified following greatest risks associated with conflicts: illicit drug trafficking (medium to high risk in most jurisdictions); proceeds from organised crime (medium to high risk); TF (low to medium risk); and sanctions evasion (low to medium risk). Other risks, such as large-scale corruption, arms trafficking, cyber-crime, the activities of foreign terrorist militants or private military companies, and human trafficking groups were typically not assessed by the majority of jurisdictions.

16. Over the last three years, some MONEYVAL jurisdictions have identified links between ML, TF and PF risks related to proceeds obtained from conflict and the use of NPOs. The abuse of NPOs has been assessed by one MONEYVAL country as a medium risk. Eight MONEYVAL jurisdictions report to have identified the NPOs being at risk to facilitate TF, however only three jurisdictions, have reviewed in more details the role of NPOs and crowd funding platforms in enabling ML, TF and PF in conflict zones. More work is required to better understand the relationship between the NPO sector and laundering proceeds obtained from conflict and/or their use for TF/PF.

17. Other risks that were referred to by respondents include: white-collar crime, fraudulent use of state subsidies, corruption, and criminal activities relating to public contracts.

1.3. Conclusion

18. Conflict generates vulnerable environment that enables obtaining criminal proceeds, sustained by corruption, hybrid warfare, cybercrime, exploitation of NPOs and other tactics/crimes. While these typologies are analysed separately in next section, their interconnection highlights the strategic nature of these financial flows and the embeddedness of illicit finance in the broader machinery of modern conflict.

19. The implications for MONEYVAL jurisdictions are significant. Many of the risks presented in this section, such as sanctions circumvention, the use of VAs, and the laundering of criminal proceeds through cross-border smuggling, are not fully addressed in current NRAs. Even where such risks are acknowledged, they are not specified and understood in depth. This gap in understanding not only weakens AML/CFT/CPF frameworks but also allows malign actors to exploit jurisdictions that perceive themselves as disconnected from external conflicts.

20. Future responses by countries should focus on integrating conflict-related risks and threats into existing risk mitigating frameworks and fostering closer collaboration with international and regional actors. FIUs and other competent authorities should deepen engagement with the private sector, leverage technological tools for tracking cross-border financial flows, and ensure that information derived from NPOs acting in conflict zones informs their risk understanding. Addressing the ML, TF and PF risks associated with conflict is not only a matter of international solidarity, but also essential to safeguarding the integrity and resilience of the global financial system.

21. AML, CFT and CPF efforts, including strategies, should target the mechanisms outlined in the section below and make more use of information gathered by the private sector and public-private partnerships (PPP), academia, think tanks, and international organisations. Being at the forefront of AML, CFT and CPF efforts, the private sector gathers large amounts of valuable data that can be used by governments to identify risks. Combining information from different sources will allow states to draw conclusions about growing risks, which will help inform future iterations of their NRAs.

2. Laundering of proceeds from conflict and/or their use for TF/PF – key emerging trends

General

22. The following section outlines the key emerging trends in the laundering of proceeds linked to conflict and/or their use for TF/PF. The section describes the most frequently observed methods, actors, and typologies across affected jurisdictions. These trends include sanctions circumvention, grand corruption, cybercrime, fraud, financing of mercenaries and private military companies, theft of material resources and assets, tax crimes, illegal gambling establishments, illegal crypto exchanges, illegal drugs trafficking, human trafficking, arms trafficking, and illegal migration.

2.1. Different methods, actors and typologies used for the laundering of proceeds from conflict and/or their use for TF/PF

Sanctions Circumvention

Sanctions Circumvention Mechanisms Involving the Democratic People's Republic of Korea

23. The UN Security Council resolutions[9] prohibit the development of technologies by the Democratic People's Republic of Korea (DPRK) for its ballistic missile programme. They also prohibit other states from co-operating with DPRK on nuclear science projects and aerospace technology.

24. However, information and case examples provided by MONEYVAL jurisdictions (see below) indicate that, despite these restrictions, certain states have continued to engage with the regime. These efforts include concealing relationships with sanctioned entities and individuals, disguising the transfer of military equipment and dual-use goods, obfuscating the nature and volume of imported tangible assets, and concealing activities related to the production and testing of weapons of mass disruption.

25. Below are cases provided by MONEYVAL members.

Case box 2

As noted by one MONEYVAL member jurisdiction, cases of proliferation-related risks have been observed in its neighbouring region. In one instance, authorities of one MONEYVAL country interdicted a foreign national arriving from a conflict zone who was suspected of involvement in the illegal movement of radioactive materials. The case, which points to possible criminal connections, is currently under investigation.

Case box 3

In another case, two companies registered in a European jurisdiction were found to be supplying oil products for military purposes to a sanctioned destination. The shipments transited through port infrastructures in specific region and, at times, through neighbouring countries to obscure their origin and circumvent sanctions. Offshore entities were used to manage both payments and logistics. Although no criminal charges were filed, national customs authorities responded by

9. UN Security Council resolutions on Democratic People's Republic of Korea (DPRK), available at https://main.un.org/securitycouncil/en/sanctions/1718#current%20sanction%20measure.

strengthening monitoring procedures and entering agreements with port operators to restrict such activities in the future.

Sanctions Circumvention Mechanisms Involving the Islamic Republic of Iran

26. Iran is subject to UN Security Council sanctions,[10] which seek to restrict the development and testing of ballistic missiles, arms transfers, and the activities of individuals associated with Iran's nuclear programme.

27. In response, Iran has adopted a range of mechanisms to circumvent sanctions, including by establishing co-operation channels with other sanctioned states to bypass traditional financial systems.

28. Below are case examples provided by MONEYVAL members.

Case box 4

One MONEYVAL jurisdiction provided the case study that is illustrative of the methods used to circumvent sanctions. The scheme used involved an offshore company controlled by an Iranian-born individual who had relocated to a neighbouring jurisdiction and sought to purchase a commercial property in Europe. The transaction was structured through a regulated trust and company service provider. Enhanced due diligence revealed that the individual operated a textile and carpet manufacturing business bearing a name noticeably similar to a sanctioned Iranian petrochemical trading firm. Further analysis indicated that the company also produced dual-use chemical goods, such as ethylene glycol, a known precursor to chemical weapons production, primarily for export to an East Asian market. The overall structure and operations raised suspicions that the entity was functioning as a front for the sanctioned company.

Case box 5

In another case submitted by one MONEYVAL member, a suspicious financial transaction amounting to approximately EUR 214 000 was flagged between an East Asian supplier and a European company, allegedly for the acquisition of sensitive microelectronics. The goods were reportedly intended for onward shipment to a second East Asian destination. The European firm's majority owner was a national of a sanctioned jurisdiction, and open-source intelligence linked the final recipient to networks associated with Iran. The transaction was ultimately halted; the goods were not exported, the funds were returned, and a criminal report was filed. This case highlights the complexity and layered nature of procurement efforts designed to circumvent formal restrictions, often involving jurisdictions and entities not themselves subject to designation.

Grand Corruption

29. In warfare settings, grand corruption facilitates the expropriation of wealth from the conflict zone, as well as redirecting resources to the benefit of supporters of the conflict. Grand corruption frequently enables also sanctions evasion by facilitating the concealment or cross-border transfer of illicit proceeds. In conflict-related contexts, this may involve the misappropriation of charitable donations through controlled foundations, or the hidden acquisition of high-value assets, such as luxury goods. The schemes used often rely on complex ownership structures and transnational

10. Resolution 2231 (2015) on Iran Nuclear Issue, available at https://main.un.org/securitycouncil/en/content/2231/background.

financial arrangements, allowing sanctioned individuals or entities to bypass restrictions and continue acquiring prohibited items.

30. Below are case studies provided by the MONEYVAL members.

Case box 6

One MONEYVAL country provided example on use of humanitarian aid as a vehicle for propaganda. In one conflict-affected region, the distribution of humanitarian assistance was controlled by conflict supporters and showcased in controlled media for narrative purposes. Independent initiatives were actively suppressed, including the detention and subsequent disappearance of a local individual who attempted to distribute the aid (food) outside of official channels.

Case box 7

Another MONEYVAL member provided case example on circumvention of sanctions through the illicit supply of luxury vehicles. A company registered in one EU jurisdiction received payment from a foreign-registered entity located outside of EU for the purchase of a high-end car, which was subsequently delivered to an individual based in Central Asia. Shortly after the export, the vehicle was registered in the sanctioned country, in direct violation of the EU's restrictive measures prohibiting the export of luxury goods. Investigations revealed that both the purchasing and selling entities were ultimately controlled by the same beneficial owner, thereby confirming the transaction as a co-ordinated attempt to evade sanctions. The individuals involved were prosecuted and received substantial financial penalties.

Cybercrime

31. Cybercrime related with conflict represents an increasingly sophisticated and systemic threat to financial and institutional stability. Cyber-attacks serve not only to compromise sensitive information but also to disrupt the functioning of public administration and critical national infrastructure, interfering with decision-making processes, service delivery, and security co-ordination. These activities are often conducted in parallel with conventional military actions and contribute directly to the degradation of a state's resilience.

32. The objectives of cybercrime in conflict settings include the obstruction of governmental systems, sabotage of essential infrastructure, theft of strategic data, dissemination of disinformation, espionage, and financial fraud. Common techniques include the distribution of malware, card cloning, phishing attacks, social engineering, manipulation of online systems (such as vishing), and the use of illegal online content. Crowdfunding platforms are also increasingly exploited to finance military objectives, including the procurement of weapons or dual-use components.

33. Below is a case example provided by MONEYVAL jurisdiction.

Case box 8

In one recent case reported by one MONEYVAL jurisdiction, a national security agency reported a sustained campaign of cyber-attacks attributed to a conflict zone. These attacks targeted the internal communication systems of various government bodies, with the aim of disrupting their operational continuity and obstructing the implementation of public policy across multiple sectors. The campaign extended to digital networks in other jurisdictions, affecting political representatives and strategic infrastructure.

Parallel investigations revealed a cybercrime group conducting ransomware attacks against over a thousand entities across multiple countries. Victims were extorted for payment in VAs, primarily cryptocurrencies, in exchange for decryption tools. Financial analysis showed significant inconsistencies between the transactions carried out by group members and their declared income levels. Transactions involved credit card activity, electronic money transfer providers, and platforms prohibited in the jurisdictions. One individual implicated in the case had no formal employment and was operating under an identity linked to a lost or stolen passport. Law enforcement authorities have launched co-ordinated transnational investigations, with financial intelligence indicating strong indicators of laundering of illicit cyber proceeds through digital channels.

34. Cybercrime in conflict contexts is therefore not only a tactical tool but also a strategic enabler of illicit financing, reinforcing the need for AML/CFT frameworks to account for hybrid threats and to develop cyber-specific typologies of financial risk.

Fraud

35. Fraudulent activity during conflict exploits institutional vulnerabilities and targets populations already suffering from displacement, shocks, and economic hardship. Conflict does not deter fraudsters; on the contrary, it creates fertile ground for new schemes to emerge, often facilitated by digital tools and weakened oversight. Fraudsters adapt their methods quickly, employing increasingly sophisticated social engineering tactics and cyber-enabled strategies to exploit both the civilian population and state systems designed to provide relief.

36. Different schemes have been observed in conflict zones, ranging from fraudulent fundraising campaigns and phishing attacks to the hijacking of social media accounts for financial extortion. Particularly vulnerable groups to these schemes include the elderly, the young, and, particularly in wartime, the families of military personnel. In many cases, fraudsters seek to access state aid that is earmarked for missing personnel or those killed in action, or to misappropriate humanitarian aid and charitable donations by pretending to be as legitimate volunteers or representatives of well-known entities. Methods used include forging attorney documents, impersonating trusted organisations, and soliciting donations for fictitious investment schemes or relief initiatives. Once obtained, funds are often laundered through a network of different accounts and converted into cash or digital currency to obscure their origin.

37. Below are case examples provided by MONEYVAL members.

Case box 9

As highlighted by one MONEYVAL member, one major case uncovered by law enforcement in conflict zone involved a transnational network of fraudulent call centres operating across several jurisdictions, with an estimated annual turnover exceeding hundreds of millions in local currency. These operations, employing thousands of individuals, used spoofed phone numbers and assumed the identities of banks, investment firms, telecommunications providers, and even government agencies to gain victims' trust. Tactics included extended multi-day phone engagements and emotionally manipulative scenarios, such as fabricated emergencies or relocation assistance, designed to extract banking credentials and persuade victims to "invest" in cryptocurrencies, stock trading platforms, or gambling returns. Although some early returns were paid out to build credibility, contact was eventually severed, and funds vanished.

Case box 10

Another MONEYVAL jurisdiction provided a case study demonstrating how fraudulent commercial activities can intersect with the evasion of sanctions. A company based in one jurisdiction was found to have acquired goods of strategic military relevance from a sanctioned state, routing payments through an intermediary shell entity registered in another jurisdiction to disguise the true origin and nature of the transaction. By deliberately avoiding the required transit licence, the company circumvented inspections and violated sanctions on the movement of military goods. Such schemes illustrate how commercial fraud and trade-based ML remain potent tools for enabling the subversion of international restrictions and the perpetuation of illicit financial flows during conflict.

Case box 11

A case example provided by one MONEYVAL member jurisdiction illustrates another typology identified by a national FIU from the analysis of suspicious transaction reports (STRs) on the use of fraudulent schemes to disguise the origin of funds and circumvent sanctions. In these cases, individuals provide false data on their residency, often using fake documents such as utility bills. VASPs or payment service providers may not verify the information or lack the means to do so, enabling the circumvention of sanctions that prohibit crypto wallet or account services for the citizens or residents of the sanctioned country.

Financing of Mercenaries and Private Military Companies

38. The financing of mercenaries and private military companies (PMCs) constitutes a critical component of conflict-related illicit financial flows. Mercenary forces and PMCs are deployed in conflict areas to secure territorial control, protect economic interests, enable regime change, or exert political influence. While some PMCs receive direct state funding, sometimes reaching hundreds of millions of euros, others rely on complex international business structures designed to obscure financial traceability and regulatory accountability.

39. The financial structures supporting these entities are diverse and opaque. Funding may originate from official government budgets, private donations, or profits from illicit trade and smuggling operations. Payments can be made via bank transfers, crypto-wallets, or in-kind compensations such as weapons, equipment, or exclusive access to exploitable natural resources. In some cases, the financial flows that sustain these groups are deliberately channelled through corporate networks operating in conflict-affected or weakly governed jurisdictions. This may involve the use of resource extraction companies engaged in gold or diamond mining, often under conditions of low transparency and limited oversight.

40. Common mechanisms for financing these entities include the illegal diversion of private investments, the misuse of NGOs or religious groups as financial conduits, the extraction of taxes or duties in occupied territories, the provision of infrastructure and services to occupying forces, and the laundering of funds through affiliated corporate entities. Additionally, unregulated currency conversion and the strategic use of VAs further complicate enforcement efforts.

41. Below is a case example provided by a MONEYVAL jurisdiction.

Case box 12

One MONEYVAL member jurisdiction provided a case study investigated by its financial intelligence unit illustrating a scheme used for financing mercenaries and private military companies.

Authorities identified a network of companies which opened bank accounts to support supplying material goods to armed groups operating in the conflict area. Financial transactions between the entities, labelled as loans, claims assignments, or industrial payments, revealed a pattern of circular fund transfers designed to obfuscate the origin and destination of the assets. Some of these funds were suspected to have been converted into cash via companies with opaque accounting practices and potential links to the trade of unregulated goods. The structure of these transactions suggests a co-ordinated effort to monetise non-cash assets in support of armed groups in conflict zones, highlighting the adaptability and reach of illicit financing methods associated with PMCs and mercenary activity.

Theft of material resources and assets

42. The appropriation of material resources and assets in conflict zones constitutes a serious breach of international law and may form part of wider patterns of crimes against humanity. The seizure of economic infrastructure, particularly plants, manufacturing facilities, and financial institutions, serves both immediate military objectives and long-term economic subjugation, effectively hindering post-conflict recovery and consolidating control over occupied regions.

43. In practice, this involves the looting of public and private assets, including banking reserves, enterprise machinery, commercial inventory, and even culturally significant property. In many cases, *ad hoc* administrative bodies are established to place seized assets under so-called "*external management*" or facilitate their re-registration under the legal frameworks of the occupying state. These measures provide a veneer of legality while enabling the exploitation of the conflict zone's industrial capacity for the purpose of the supporting the conflict.

44. Below is a case example provided by a MONEYVAL member.

Case box 13

One illustrative case shared by one of the MONEYVAL member jurisdictions revealed how the facilities of an industrial plant located in a conflict zone were commandeered and repurposed in support of military objectives using complex schemes. In this case, the plant was re-registered under another legal system and partially dismantled, with assets transferred across the border. It continued operations locally, functioning as a logistics and repair base for armed groups and regular military forces of the occupying state. The director of the plant was further linked to a foreign-registered company involved in the procurement and assembly of military-grade equipment, including unmanned aerial vehicles used in artillery and missile targeting operations. This company also served as a conduit for the import of dual-use goods under the guise of civilian manufacturing, thereby circumventing international sanctions.

A constellation of non-resident companies was created to conduct cross-border financial transactions, and these vehicles were also used by sanctioned individuals, illustrating how asset theft, tax fraud, and sanctions evasion may converge in conflict-affected contexts.

Tax Crimes

45. Tax crimes represent a pervasive and damaging trend in conflict-affected environments, undermining state revenue at a time when public expenditure and resilience are most critical. In conflict zones, tax infrastructure is often dismantled or repurposed to serve the fiscal needs of conflict initiator, while in non-occupied areas, the strain of conflict impairs the state's ability to detect, deter and prosecute complex tax evasion schemes. These schemes are not limited to domestic actors;

transnational networks often exploit legal loopholes, double taxation treaties, and cross-border payment systems to launder illicit proceeds while depriving states of vital tax income.

46. Among the most prevalent methods for tax crimes are the generation of fictitious invoices, the use of absent traders, and the manipulation of legitimate enterprises for shell activities. Transactions are often structured to appear as legitimate activities related to service provision, such as passenger transport or consultancy; in some instances, these arrangements make use of well-known online ticketing platforms or digital marketplaces that dominate regional sectors, further complicating detection.

47. Below are case examples provided by MONEYVAL jurisdictions.

Case box 14

Case 1: One MONYEVAL member jurisdiction provided case study on the use of an online transport booking platform controlled through a complex chain of corporate ownership across multiple jurisdictions, including offshore entities and companies domiciled in sanctioned countries. The platform acted as an intermediary to channel funds from ticket sales through a series of false service contracts and manipulated financial flows, eventually transferring the proceeds out of the country. These funds were then routed through other entities, implicating a broader tax fraud scheme aimed at funding military operations in conflict zones.

Case 2: In another instance, a domestic agricultural exporter engaged in transactions with a foreign non-resident company under a contract that was later found to bear forged seals and digital signatures. No payment was ever credited for the exported goods, nor were the corresponding tax liabilities declared. The foreign counterparty was revealed to be an entity operating outside the trade sector entirely, serving instead as a financial conduit for unrelated service transactions. The produce was subsequently sold to legitimate grain traders, and the earnings redirected into external payment circuits, bypassing both fiscal control and currency regulation.

48. These operations are often facilitated by the misuse of international legal instruments, such as bilateral tax treaties, or by exploiting online payment systems not subject to national regulatory scrutiny. In many cases, the financial structuring is explicitly designed to mask the beneficial ownership of the involved companies, while obscuring the origin and final use of the funds. The deliberate layering of transactions across multiple jurisdictions not only enables the laundering of tax fraud proceeds but also aligns with wider schemes of sanctions evasion.

Illegal Gambling Establishments

49. The operation of illegal gambling establishments and the misuse of licensed gambling platforms continue to present serious vulnerabilities to AML and CFT systems, particularly in jurisdictions with weak supervisory frameworks due to conflict. As highlighted in joint typological research by international standard-setting bodies, including the FATF and regional counterparts, the gambling sector remains exposed to abuse due to structural features such as cash-intensity, cross-border payment channels, and the involvement of opaque ownership structures.

50. One prevalent technique involves the diversion of player payments through merchant codes falsified by co-operating financial institutions, thereby masking the true nature of transactions. These misclassified payments are registered as unrelated goods or services and processed by banks that simultaneously manage payroll and administrative costs for the gambling establishment, reducing the likelihood of detection. The funds accumulated in this manner are used to disburse untaxed winnings and generate “black non-cash money,” with the remainder being absorbed by the operators as undeclared profits.

51. These profits may subsequently be transferred abroad, bypassing taxation and supervision. In cases where the gambling operators maintain relationships with entities supporting conflict, such funds may ultimately support activities linked to armed conflict or broader destabilisation efforts.

52. Below is a case study provided by MONEYVAL member.

Case box 15

One MONEYVAL jurisdiction provided case study illustrating misuse of gambling operator in conflict zone. A national gambling oversight authority conducted inspections of land-based gambling operators across six entities, revealing significant deficiencies in staff training for the detection and growth of suspicious transactions. Although many online operators employed automated systems for identifying red flags, staff at physical venues demonstrated limited awareness of indicators of ML/TF, undermining the effectiveness of internal control systems. Administrative sanctions, totalling over EUR 63 000, were imposed for breaches of applicable AML/CFT/CPF legislation, and remedial training was mandated to strengthen frontline awareness. This case highlights both the technical sophistication of financial manipulation schemes in the gambling sector and the continued need for robust supervision, enforcement, and capacity-building among operators, particularly in environments vulnerable to misuse.

Illegal Crypto Exchanges[11]

53. New technologies, including VAs and cryptocurrency-based financial services, create new opportunities for the generation and laundering of illicit proceeds in conflict environments. Cryptocurrencies are frequently used to circumvent sanctions, finance subversive or terrorist activities, and facilitate transactions linked to the illegal arms, narcotics, and gambling markets. Their ability to anonymise transactions and bypass official controls enables the accumulation of proceeds that are difficult to trace and often transnational in scope.

54. Case examples provided by one MONEYVAL jurisdiction demonstrate that that these criminal activities often involve significant amounts of money and complex schemes.

Case box 16

One MONEYVAL jurisdiction provided information on a notable case involving a VASP operating globally under a single brand but structured through legal entities registered in multiple jurisdictions. This exchange laundered funds and facilitated sanctions evasion for multiple high-risk exchanges and darknet platforms involved in illegal trade and cybercrime. The platform received assets from unlicensed peer-to-peer (P2P) and over-the-counter exchanges, operating across various countries, and converted these into fiat currency through banking systems, including those of sanctioned financial institutions. The platform's ownership structure featured politically exposed persons and nominees suspected of laundering proceeds from illegal gambling operations and previously identified financial crime schemes.

Between 2019 and 2022, the platform received hundreds of millions of USD in VAs from sanctioned exchanges and darknet sources. Several of these transactions originated from jurisdictions with high ML/TF risk and were linked to state-affiliated hacker groups and sanctioned peer-to-peer intermediaries. Blockchain analysis revealed that VAs flowed from sources connected to illicit cyber activity, sanctioned trading platforms, and unregulated exchanges. Open-source information

11. See also MONEYVAL typologies paper on *Practice of Using Virtual Assets, Virtual Asset Service Providers & Platforms in the Laundering of Criminal Property*, available at https://www.coe.int/en/web/moneyval/activities/typologies (note: will be published in January 2026).

further indicated a pattern of reduced scrutiny and law enforcement activity following changes in ownership, raising concerns over regulatory capture and concealment.

Suspicious activity reports and transaction monitoring data indicated that large sums were transferred into the platform's accounts, allegedly for the provision of services, from companies involved in illegal gambling and conversion schemes. The documentation used to justify these transactions is suspected to have been falsified to launder criminal proceeds. The case illustrates the use of VAs, layered ownership, and peer-to-peer infrastructures to enable the movement and concealment of funds in the context of conflict-related financial crime. A pre-trial investigation is ongoing.

Case box 17

As documented by one MONEYVAL country in its report, in 2024, a national Financial Crime Investigation Service levied a record fine of EUR 9.3 million against a national-registered VASP. The Service found that the VASP facilitated transactions for clients of a different country, including those from sanctioned banks, through its platform. The company continued activities incompatible with international sanctions, including: allowing transactions with sanctioned banks; providing cryptocurrency wallet, account management, or custody services to individuals from that country and entities; failing to properly identify and verify clients to avoid losing revenue; not terminating transactions with sanctioned banks, and other deficiencies in internal policies and control procedures related to customer identification, risk assessment, and reporting.

Illegal Drugs Trafficking

55. Drug trafficking remains a significant source of proceeds in conflict and post-conflict environments. Conflict disrupts existing enforcement structures and can alter established trafficking routes, either by opening new corridors or rerouting flows away from zones of intense fighting. Such instability facilitates the operations of organised criminal groups, which adapt swiftly to shifts in territorial control, security presence, and border management. Conflict-affected regions may become key transit zones for narcotics, enabling access to lucrative markets in neighbouring jurisdictions.

56. Below is a case example provided by MONEYVAL jurisdiction.

Case box 18

Drawing on the experience of one MONEYVAL member, recent seizures illustrate the emergence of new transit routes linking conflict-affected or unstable regions to broader drug distribution networks. In one case, nearly 700 kilograms of cocaine destined primarily for the European market were seized in a capital city of a large Eurasian country. Additional shipments, including hundreds of kilograms of narcotics hidden within fruit consignments, were intercepted in another major metropolitan area. These developments reflect both increasing domestic demand in urban centres and an adaptation of trafficking strategies in response to improved controls at traditional maritime entry points into Europe. Such shifts in trafficking patterns underscore the nexus between conflict, organised crime, and the generation of proceeds from illegal markets.

Human Trafficking

57. Human trafficking constitutes a major source of criminal proceeds in conflict zones, driven by the large-scale displacement of vulnerable populations and the collapse of law enforcement and protection systems. Conflict creates conditions in which individuals, particularly refugees, children,

and former military personnel, become targets of trafficking for sexual exploitation, forced labour, forced begging, or unlawful adoption. The limited capacity of receiving states to register and monitor incoming displaced persons increases the risk of exploitation by organised criminal networks operating in or near the conflict zone. Reports also indicate the existence of illicit labour markets, and in some cases, the illegal recruitment of civilians and ex-combatants into paramilitary roles.

58. In parallel, criminal groups operating under the direction of hostile actors have used forged documentation to create charitable organisations as fronts for financial and operational support. These entities collect funds under the pretext of humanitarian aid, which are then redirected to support terrorist plots or subversive activities, including attacks on critical infrastructure. The laundering of funds under the guise of humanitarian support has also been documented, with large cash withdrawals occurring in jurisdictions separate from the origin of the transfers. Complex multi-jurisdictional corporate structures have additionally been employed to obscure beneficial ownership and conceal the source and intended use of illicit proceeds, including the financing of weapons transfers and military equipment. These cases illustrate the convergence of human trafficking, TF, and sophisticated laundering schemes within conflict-affected environments.

Arms Trafficking

59. The illicit trade in arms and ammunition is a critical threat in conflict zones, where weakened regulatory controls and the collapse of border and customs enforcement enable the circulation of weapons outside legal oversight. Conflict environments allow weaponry to move rapidly into the hands of unauthorised entities, including paramilitary groups and organised criminal networks. These arms flow often intensify other threats to national and regional security, including increased criminality, terrorism, and inter-group violence. Experience from multiple jurisdictions indicates that weapons initially used in theatres of conflict are often smuggled into criminal markets in surrounding or third countries.[12]

60. The global arms market supporting these transfers operates through both financial and barter-based mechanisms, often mediated via opaque corporate structures. Conflict-affected jurisdictions, particularly those under embargo or restrictive measures, may use foreign-flagged operations, shipping through secrecy jurisdictions, and shell companies to obscure the origin and destination of arms transfers. Offshore entities may be employed to facilitate the purchase and shipment of military-grade weapons, circumventing embargoes or international restrictions. Such arrangements often involve conflict profiteering networks and raise serious concerns regarding the use of transnational corporate secrecy to enable violations of international sanctions and the financing of conflict.

Illegal Migration

61. Armed conflict is a recognised driver of irregular migration, which frequently involves the undocumented movement of individuals across international borders. While many of these individuals are refugees fleeing violence and instability, such movements can create vulnerabilities that are exploited by organised criminal networks, including for the purposes of smuggling, trafficking, terrorist recruitment, and forced participation in paramilitary or mercenary operations. In conflict-related contexts, individuals without legal status may be coerced into participating in military activities or subjected to blackmail and extortion. The systemic exploitation of migrants not only generates proceeds for those who enable and control such flows but also raises broader national and regional security concerns.

12. The trade in illegal firearms and explosives (Europol), available at https://www.europol.europa.eu/crime-areas/trade-in-illegal-firearms-and-explosives.

62. Below is a case study provided by MONEYVAL member.

Case box 19

For instance, in one documented case provided by a MONEYVAL member country, tens of thousands of migrants who had received citizenship in a particular jurisdiction were later detained and allegedly forced into military participation in an ongoing armed conflict. Authorities reported that thousands were actively deployed to the conflict zone, often following targeted legal harassment campaigns intended to coerce enlistment in exchange for avoiding arrest or expulsion. Such practices emphasise how migration-related vulnerabilities may be deliberately weaponised to support conflict objectives and contribute to the destabilisation of both origin and recipient states and highlight the role of migration-linked exploitation in the broader architecture of conflict-related proceeds.

2.2. Conclusion

63. The laundering of proceeds from conflict is characterised by operational complexity, transnational reach, and integration into both formal and informal financial systems. The section has outlined how conflict facilitates the generation of illicit funds through a wide array of predicate offences, including corruption, trafficking, fraud, and the misappropriation of resources. These proceeds are channelled through layered schemes involving corporate structures, digital assets, and cross-border networks, often with the support or acquiescence of state-linked actors.

64. Identified typologies confirm the use of hybrid mechanisms such as the sanctions circumvention through offshore entities, financing of private military companies and the exploitation of humanitarian and non-profit structures. Common features include the manipulation of ownership chains, the obfuscation of fund origin, and the use of high-risk jurisdictions. These findings indicate that conflict-related financial flows operate across multiple vectors simultaneously, reinforcing their strategic and systemic nature.

65. The typological material presented reflects recurring patterns in the laundering of conflict-derived proceeds, with emphasis on geographic spillover, regulatory evasion, and the sustained use of adaptive financial infrastructures. Collectively, these elements illustrate the role of financial crime as an enabler of armed conflict and destabilisation.

3. Risk mitigation measures

General

66. This section provides an overview of global and regional AML, CTF and CPF measures in the context of armed conflict. It examines relevant actions taken by MONEYVAL member jurisdictions to mitigate ML and illicit financing risks arising from such environments, with a focus on typologies associated with conflict.

3.1. Overview of global and regional AML/CFT/CPF measures in the context of armed conflict

International Sanctions Policy

67. Sanctions constitute an established instrument of international influence, particularly in response to terrorism and conflict. They have proven effective in restricting access to resources that may be used to finance armed conflicts, while simultaneously imposing economic and political constraints on decision-makers and elite networks within the targeted jurisdictions.

68. The implementation of sanctions regimes has a direct bearing on national AML/CFT/CPF systems. In jurisdictions enforcing sanctions, not only governments but also private sector entities and individuals are legally required to ensure that financial transactions are subject to adequate supervision and meet the relevant standards for AML and counter-illicit financing compliance.

UN Security Council Sanctions

69. The United Nations Security Council maintains the authority to impose sanctions as part of its mandate[13] to preserve international peace and security under Chapter VII of the UN Charter. Sanctions measures adopted under Article 41 encompass a variety of enforcement tools that do not involve the use of armed force.

70. At present, there are 15 active UN sanctions regimes addressing issues such as conflict resolution, non-proliferation, and counterterrorism. Each regime is managed by a sanctions committee chaired by a non-permanent member of the Security Council, with support from 11 monitoring groups, panels, and teams covering 12 of the 15 committees.

71. In parallel, the UN has adopted an international legal instrument against the recruitment, use, financing, and training of mercenaries, further contributing to the global legal framework aimed at mitigating the financing of armed conflict.[14]

European Union Restrictive Measures

72. The European Union (EU) applies restrictive measures ('sanctions') in support of its Common Foreign and Security Policy objectives.[15] These include conflict prevention and resolution, counterterrorism, the non-proliferation of weapons of mass destruction, and the promotion of democracy, the rule of law, and human rights. EU sanctions establish binding legal obligations for all EU citizens and operators, as well as for any financial institutions and businesses operating within the European Union.

13. UN Security Council sanctions, available at https://main.un.org/securitycouncil/en/sanctions/information.
14. UN International Convention against the Recruitment, Use, Financing and Training of Mercenaries, available at www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-against-recruitment-use-financing-and.
15. European Union sanctions, available at www.eeas.europa.eu/eeas/european-union-sanctions_en.

73. The implementation of EU sanctions is decentralised and carried out at the level of individual Member States. While the European Commission does not function as a central supervisory authority, it plays a co-ordinating and supportive role. This includes monitoring the consistent application of sanctions, assessing their effectiveness, and developing methodological tools such as interpretative guidance, explanatory materials, and frequently asked questions to support implementing entities.

74. In practice, EU restrictive measures may take the form of financial sanctions, including asset freezes, which can apply to both public and private sector actors. Credit and financial institutions bear particular responsibility for enforcing these obligations, as they are directly involved in the execution of most financial transactions.

75. Violations of sanctions regimes are criminalised in the majority of EU Member States,[16] with penalties that range from administrative fines to custodial sentences. Directive (EU) 2024/1226 intends to establish minimum rules concerning the definition of criminal offences and penalties for the violation of those Union restrictive measures. Fines for individuals vary by jurisdiction, from EUR 1 200 in one jurisdiction to EUR 5 million in another, while corporate fines range from EUR 133 000 in one case to EUR 37 million in a third jurisdiction. The enforcement of these provisions is subject to national prosecutorial discretion and depends on the authority and capacity of Member States to monitor compliance.

Other measures

FATF

76. The Financial Action Task Force (FATF) serves as the international standard-setter for AML/CFT/CPF measures, promoting the implementation of legal, regulatory, and operational frameworks aimed at safeguarding the integrity of the global financial system.[17] While FATF's mandate does not encompass international humanitarian law and does not include standards related to states' engagement in armed conflicts, the organisation plays a critical role in addressing conflict-related risks to financial security.

77. The FATF standards apply in all circumstances, including during armed conflict. FATF guidance explicitly states that countries must continue to identify, assess, and mitigate ML, TF and PF risks, even when facing aggression. In practice, however, states involved in conflict may find their capacity to enforce AML/CFT measures significantly diminished. At the same time, the opportunities for criminal activities arising from conflict may be exploited to finance activities fuelling the conflict itself. Serious organised crime groups can also take advantage of such situations.

MONEYVAL

78. MONEYVAL's activities in this area are aligned with FATF policy and guidance.[18] The Committee works to ensure that its member jurisdictions maintain effective mechanisms to combat ML and TF, in line with established international standards. Compliance is assessed through the mutual evaluation process, which includes a peer review of legal, financial, and law enforcement frameworks.

79. MONEYVAL's current strategic direction is set out in its 2023–2027 Strategy,[19] adopted on 25 April 2023, alongside the Declaration of Ministers and High-level Delegates of the Member States and

16. Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis www.eurojust.europa.eu/sites/default/files/assets/genocide_network_report_on_prosecution_of_sanctions_restrictive_measures_violations_23_11_2021.pdf.
17. FATF Homepage, available at www.fatf-gafi.org.
18. MONEYVAL Homepage, available at www.coe.int/en/web/moneyval/.
19. MONEYVAL Strategy 2023-2027, available at https://rm.coe.int/moneyvalstrategy2023-2027-en/1680ab0b06

Territories of MONEYVAL.[20] These documents reaffirm the Committee's commitment to addressing the laundering of criminal proceeds, the financing of terrorism, and the financing of weapons proliferation, including in the context of armed conflict.

Egmont Group

80. The Egmont Group plays a central role in facilitating international co-operation and secure information exchange between national FIUs.[21] Its primary objective is to support the development of a global AML/CFT framework grounded in mutual trust and collaboration.

81. In the context of armed conflict, the Egmont Group has taken concrete measures to safeguard its operational integrity. This has included suspending the membership of FIUs supporting conflict and revoking their access to the Egmont Secure Web platform.

3.2. Examples of sanctions relating to illegal financial proceeds from conflict

82. Sanctions serve as a key mechanism for degrading military capabilities and limiting the escalation or spread of conflict. An examination of how such measures are applied and enforced contributes to the development of more targeted and effective policy responses. This section provides examples of conflict-related sanctions applied by a MONEYVAL jurisdictions.

Case box 20

A MONEYVAL member jurisdiction reported that special economic and other restrictive measures, both individual and sectoral, may be imposed to protect national interests, national security, and territorial integrity. Decisions regarding the imposition, modification, or lifting of sanctions are made by the competent national security authority and enacted by presidential decree.

To date, this jurisdiction has sanctioned over 17 000 individuals and legal entities. On 9 October 2022, a presidential decree implemented a decision introducing or amending targeted special economic and other restrictive measures (sanctions), which imposed sanctions on 2 251 individuals. Among those targeted were financial institutions, including domestic affiliates of large foreign banks.

Case box 21

As shown in data from one responding jurisdiction, further measures were adopted on 22 February 2023, when the national parliament approved a resolution enacting a decision on the application of sectoral special economic and other restrictive measures to financial institutions operating in or associated with a designated jurisdiction. This was implemented through a presidential decree. The decision introduced sanctions for a period of 50 years targeting all banks registered or operating in the relevant foreign state, including its central bank, along with all associated non-bank credit institutions, payment system operators, insurance companies, investment funds, and other financial institutions.

These sanctions include a suspension of transactions involving the assets of designated financial institutions, a prohibition on establishing or maintaining business relationships with them, and a

20. Declaration of Ministers and high-level delegates of the member States and territories of MONEYVAL, available at https://rm.coe.int/moneyval-2023-hldeclaration-en/1680ab0ae3.
21. The Egmount Group Homepage, available at: https://egmontgroup.org.

ban on fulfilling economic or financial obligations in their favour. In addition, the measures prohibit the crediting of funds to clients' accounts, whether individuals or legal entities, when transfers are initiated using electronic payment instruments issued by financial institutions of the targeted jurisdiction.

Case box 22

Another MONEYVAL jurisdiction reported instances where, in June 2025, one jurisdiction approved legislative amendments to its Law on Restrictive Measures in response to military aggression against another country. This establishes a national legal framework allowing to impose individual and economic sanctions on the aggressors – specifically asset freezes and sectorial restrictions – even in cases where EU-wide sanctions are not present or extended. Two jurisdictions already have a legal basis for national restrictive measures (individual and sectoral), and another country is also considering introducing such legal basis in its national legislation.

3.3. The practice of blocking, suspending, or freezing conflict-related transactions and assets

83. A number of jurisdictions have applied asset freezes, suspensions, and seizures as part of broader efforts to enforce sanctions and limit the financial flows associated with armed conflict. These measures target individuals and entities directly or indirectly linked to military aggression or violations of international law. They often involve the blocking of transactions, the freezing of bank accounts and corporate assets, and the seizure of high-value property, including real estate and transport vessels.

84. Below are case examples provided by MONEYVAL jurisdictions.

Case box 23 – Case examples of freezes, suspensions, and seizures to enforce sanctions

Case 1: According to the national authorities of one MONEYVAL jurisdiction, assets amounting to EUR 212 000 were frozen, while another reported a freeze of EUR 147 000. A local court in a third jurisdiction ordered the freezing of over approximately EUR 6 billion in assets linked to a sanctioned individual.

Case 2: Elsewhere, more than EUR 20 million were frozen, with over 90% of the assets connected to designated individuals, including EUR 11,7 million in financial institutions and EUR 8,4 million in tax and customs prepayment accounts.

Case 3: Another jurisdiction implemented asset freezes against individuals and companies identified by international partners as having facilitated sanctions evasion.

Case 4: As reflected in the contribution submitted by one member, approximately EUR 80 million were frozen across banks, affecting 35 companies and six individuals. One private financial institution froze assets of clients totalling approximately EUR 274 million, while another jurisdiction blocked assets valued at over EUR 103 million. Equivalent procedures were adopted in line with regional practice, swiftly implementing asset freezes and sanctions.

Case 5: A case presented by one MONEYVAL jurisdiction demonstrates that, assets exceeding EUR 1 billion were seized, including shares in three companies placed under temporary management to prevent ownership transfers.

Case 6: Another jurisdiction froze assets valued at up to approximately EUR 392,1 million, including state-owned foreign properties on its territory as of late 2023.

Case 7: In a separate case, nearly approximately EUR 870 million in foreign assets were frozen.

Case 8: In the example provided by one member jurisdiction, sanctions in the form of asset blocking were imposed on over 10 000 individuals associated with conflict. Authorities also arrested and froze assets valued at around EUR 6 500 belonging to an enterprise partially owned by a foreign national. The enterprise was allegedly involved in tax evasion and the transfer of funds abroad through fictitious transactions. The seized corporate rights and real estate were transferred to the competent national asset management agency. Additional measures include the impoundment of a foreign oil tanker under international sanctions and the seizure of a 300-foot yacht belonging to a designated individual in a port city

Case 9: Another jurisdiction aligned with international sanctions, freezing the assets of 34 foreign nationals, including politicians and officials, and targeting properties held within its territory.

3.4. Application of confiscation to conflict-related assets of sanctioned persons

85. The application of confiscation measures to assets held by sanctioned individuals linked to conflict represents a growing area of enforcement. Several jurisdictions have implemented legal mechanisms enabling the permanent transfer of such assets into state ownership, often relying on specific sanctions legislation or anti-corruption procedures.

86. Below is a case example provided by MONEYVAL jurisdiction.

Case box 24 – Case examples of confiscation of conflict-related assets

Case1: One MONEYVAL member jurisdiction's response indicated that the Ministry of Justice has exercised its powers under national sanctions legislation by submitting 58 lawsuits to a specialised anti-corruption court since May 2022, seeking the confiscation of assets held by sanctioned individuals. A detailed public register of these confiscated assets, including case references and identifying information, has been made available through the competent state authority. Since the escalation of the conflict, assets valued at the equivalent of at least approximately EUR 307 149 450 have been confiscated. These include properties associated with several sanctioned individuals, as well as others identified as collaborators or former officials. A total of 1 175 assets with a book value of EUR 270 million were transferred to the state asset management body, along with approximately EUR 589 million in bank deposits and approximately EUR 830 000 million in claim rights.

Case 2: As emerging from one MONEYVAL jurisdiction's reporting, an additional ruling issued in January 2023 by the same anti-corruption court applied the confiscation of assets located in the jurisdiction and linked to a sanctioned individual identified as a former executive of a large state-owned enterprise. The ruling relied on provisions of the national sanctions law that allow for the transfer of such assets into public ownership.

Case 3: Based on the insights shared by one member jurisdiction, authorities imposed both financial and confiscatory sanctions on a domestic company for violations of international sanctions, including unauthorised transactions involving entities in multiple foreign jurisdictions. The company was fined EUR 13 618 175, and six tractor semi-trailers used in the transaction were confiscated. The enforcement action followed a determination by customs authorities that the transactions constituted a breach of sanctions regulations.

Case 4: As reported by another MONEYVAL member authority, in September 2023, some EU jurisdictions banned vehicles with license plates from a sanctioned country from entering their territories, following an EU Frequently Asked Questions on the implementation of sanctions. The new regulation of one of those jurisdictions also required vehicles already inside its territory to be re-registered locally or to be removed from the country. In March 2024, national authorities enforced this rule by seizing their first vehicle (worth EUR 41 000) at border crossing; within September of 2024, 66 vehicles were denied entering their territories.

Vehicles are considered economic assets and could be sold, transferred or otherwise used to generate value in the EU. Sanctions enforcement can extend beyond traditional finance, targeting assets (like vehicles) that may otherwise serve as channels for preserving or moving wealth.

3.5. Case law in the area of conflict-related sanctions policy

87. Judicial proceedings play a key role in enforcing conflict-related sanctions, providing legal precedent and reinforcing the operational effect of restrictive measures. Recent cases in MONEYVAL jurisdictions illustrate how national courts have applied sanctions legislation to confiscate assets or penalise violations of sanctions regimes.

88. Below are case examples provided by MONEYVAL countries.

Case box 25 – Case law examples related to conflict-related sanctions

Case 1: According to accounts from one MONEYVAL member authority, a national anti-corruption court upheld a claim brought by the Ministry of Justice for the confiscation of property belonging to a sanctioned individual identified as a key financial supporter of a conflict. The asset in question, a large fishing trawler under construction at the time of the conflict escalation, was valued at over the equivalent of approximately EUR 20 million. The vessel was found to be part of a commercial fleet controlled by the sanctioned person, whose business activities contributed significantly to supporting the conflict. Ownership of the asset had been concealed through registration under a front company. The national security services uncovered the concealment scheme and secured the freezing and subsequent nationalisation of the vessel.

Case 2: As reported by another MONEYVAL jurisdiction, a court ruled on a sanction's violation involving a resident of foreign origin who attempted to export three luxury vehicles (Mercedes-Benz, Audi, and BMW) to a sanctioned destination, in contravention of applicable export restrictions. The export of high-value vehicles to that jurisdiction had been prohibited under EU sanctions adopted in early 2022. The individual was convicted and fined the equivalent of approximately EUR 11 500 and was further prohibited from engaging in motor vehicle sales for a period of 20 months. Additionally, the court ordered the repayment of approximately EUR 132 000, representing advance payments received from clients in the sanctioned destination. The ruling has entered into force.

3.6. Strategic documents

89. Armed conflicts have demonstrated the need for enhanced and co-ordinated international efforts to mitigate the risks posed by illicit financial flows that sustain or facilitate violence. Across MONEYVAL jurisdictions and beyond, a number of strategic responses have emerged that reflect both progress and persistent implementation challenges. These responses generally focus on strengthening legislative and institutional frameworks, improving co-ordination, and integrating conflict-related

threats into national risk assessments and operational planning.

90. A common good practice is the development or revision of national AML/CFT/CPF strategies to account for emerging risks linked to armed conflict. Several jurisdictions have updated their strategic frameworks to align with international standards, incorporating measures such as enhanced customer due diligence, the inclusion of conflict-related risk typologies, and stronger oversight of transactions involving high-risk geographies. Others have formalised interagency co-ordination mechanisms, such as task forces, national working groups, and AML/CFT partnerships, that include both public authorities and private sector actors. These structures support the implementation of targeted sanctions, export controls, and financial transaction monitoring.

91. Monitoring and enforcement tools are being strengthened in some jurisdictions, with financial intelligence units launching targeted screening of cross-border transactions or proactively identifying sanctioned entities. Risk assessment processes have also been expanded to consider proliferation financing and the misuse of financial channels to support the acquisition of dual-use goods. In jurisdictions where national risk assessments are underway or recently completed, action plans are being prepared to operationalise their findings, often with a focus on sanctions implementation and international co-operation.

92. However, implementation remains uneven. While some countries have advanced risk-based approaches and integrated military conflict considerations into their national strategies, others are still in the planning phase or have limited institutional co-ordination. The decentralised application of sanctions, reliance on voluntary information sharing, or limited engagement with the private sector may undermine the effectiveness of strategic frameworks.

93. In response to these observations, it is proposed that MONEYVAL member jurisdictions consider developing specific action plans addressing ML/TF/PF risks arising from armed conflict, as part of their upcoming NRAs. These plans should include co-ordination mechanisms, sectoral guidance, and integration of conflict-related indicators into supervisory, investigative, and policy functions.

3.7. Conclusion

94. The measures reviewed in this chapter demonstrate a broad recognition of the financial risks associated with armed conflict and the increasing sophistication of state and institutional responses. A range of mechanisms – legal, regulatory, operational – has been deployed to detect, disrupt, and deter the laundering of proceeds and the financing of destabilising activities, particularly in the context of sanctions enforcement and cross-border co-operation. Confiscation, asset freezing, and financial intelligence co-ordination have emerged as central tools across jurisdictions.

95. Nevertheless, responses remain uneven, and challenges persist in the consistent implementation, supervision, and risk integration of conflict-related threats. Gaps in interagency co-ordination, the limited use of proactive financial intelligence, and varying national practices on sanctions monitoring can affect the effectiveness of current frameworks. Moreover, while some jurisdictions have developed robust strategic planning instruments, others are still in the early stages of integrating conflict dynamics into AML/CFT/CPF risk management.

96. Going forward, the operationalisation of conflict-related financial risk mitigation should be strengthened through structured action plans, more systematic data exchange, and the alignment of financial supervision with geopolitical risk analysis. MONEYVAL member jurisdictions are encouraged to continue refining their approaches, ensuring that national systems are equipped to anticipate, assess, and respond to the financial dimensions of armed conflict in a timely and co-ordinated manner.

www.coe.int/MONEYVAL

December 2025

Typologies report

MONEYVAL

Typologies Report

Money Laundering, Terrorism Financing and Proliferation Financing Risks and Trends Linked to Proceeds Obtained from Conflicts

This typology research examines how conflicts create conditions for obtaining the illicit proceeds, how they are laundered and/or used for TF/PF. The project identifies the relevant patterns, trends and vulnerabilities to strengthen anti-money laundering, combating financing of terrorism and proliferation financing frameworks and international co-operation.