Center of Excellence in
Anti-Money Laundering

Financial Integrity as Security: The Role of AML/CTF, Fraud Prevention and Sanctions in National and Collective Defence

Center of Excellence in Anti-Money Laundering

Policy Paper

May 2026
Vilnius

Executive Summary

Financial systems have become a central domain of modern security competition. Financial crime — including money laundering, terrorist financing, large-scale fraud and sanctions evasion — is no longer a standalone compliance issue, but a key enabler of broader security threats, from hybrid operations to the circumvention of restrictive measures.

This paper argues that financial integrity must be treated as a core pillar of national and collective security. AML/CTF frameworks, fraud prevention and sanctions implementation together form an integrated preventive security layer that limits hostile actors' access to financial systems, increases the cost of illicit activity and enables early detection and disruption of threats.

The analysis shows that these mechanisms are deeply interconnected. Money laundering techniques facilitate sanctions evasion and the concealment of illicit networks; fraud generates significant revenues that sustain organised crime and undermine economic stability; and weaknesses in sanctions enforcement create strategic vulnerabilities comparable to gaps in cyber or border security. In hybrid threat environments, these dynamics converge, allowing financial systems to be exploited for strategic effect without the use of conventional force.

At both European and national levels, this perspective is increasingly reflected in policy frameworks. The European Union's economic and security strategies recognise the growing link between financial systems and security outcomes, while Lithuania's National Security Strategy highlights the importance of preventing illicit financial flows and strengthening economic resilience. This convergence underscores the need to move beyond a narrow compliance-based approach and to embed financial integrity within the broader security architecture.

The effectiveness of this approach depends not only on regulatory design, but on implementation. Risk-based supervision, timely information exchange, effective sanctions enforcement and close cooperation between public authorities, financial institutions and international partners are critical to ensuring that financial systems can function as a preventive layer of defence.

The findings of this paper lead to a clear conclusion: financial systems must be treated as part of the first line of defence. Strengthening AML/CTF measures, advancing fraud prevention and ensuring robust sanctions implementation are not only regulatory priorities, but essential security functions that directly contribute to national and collective resilience.

Center of Excellence in
Anti-Money Laundering

INTRO

Economic and financial systems have become a central arena of modern security competition. As recognised in the European Union's approach to economic security, financial flows, dependencies and regulatory loopholes are increasingly exploited as instruments of geopolitical pressure and hybrid warfare. The EU Security Union Strategy further highlights that threats — including organised crime, terrorism, cyber risks and financial crime — are interconnected and mutually reinforcing, making financial crime a critical enabler of broader security risks and reinforcing the need to treat financial integrity as a core pillar of European security[1].

This perspective is also reflected at the national level. Lithuania's National Security Strategy recognises that threats increasingly emerge not only from military or cyber domains, but also from economic and financial activities, underscoring the importance of preventing illicit financial flows and strengthening resilience[2]. In this context, money laundering, terrorist financing, large-scale fraud and sanctions evasion are not isolated phenomena, but mechanisms used to finance aggression, bypass restrictive measures, distort markets and undermine democratic resilience — with weak enforcement creating vulnerabilities comparable to failures in cyber or physical defence.

Against this backdrop, this document proceeds from the position that AML/CTF frameworks, fraud prevention and sanctions implementation constitute core elements of national and collective security, requiring coordinated action across public authorities, the financial sector and international partners.

AML/TF as a Pillar of National and Collective Security

AML/TF frameworks are most often approached as regulatory safeguards designed to prevent criminal abuse of the financial system. Assessed through a national security lens, however, their function is broader and more strategic: AML/TF measures protect the integrity of financial infrastructure and constrain the ability of hostile actors—state and non-state—to access, move and deploy resources in support of destabilising activities. This perspective is consistent with Lithuania's National Security Strategy, which recognises that threats to national security increasingly arise from economic and financial activities and emphasises the need to prevent illicit financial flows and strengthen systemic resilience[3].

This security logic is reflected in the evolution of international standards. The mandate of global standard-setters has progressively expanded[4] from money laundering to terrorist financing and the financing of weapons of mass destruction. This expansion is not technical but strategic. Terrorist financing and proliferation financing are internationally recognised threats to peace, state sovereignty and global stability, and financial controls are designed to deny these actors access to the legitimate financial system at scale.

The link between AML/TF and international security is particularly explicit in the context of counter-terrorist financing and non-proliferation. Terrorism and its financing have been formally treated as threats to international peace and security, establishing a clear normative basis for financial controls as

[1] European Commission (2020), *EU Security Union Strategy: a new security ecosystem*, IP/20/1379, 23 July 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[2] Lithuanian Parliament (Seimas), *National Security Strategy of the Republic of Lithuania*, Resolution No. IX-907 of 28 May 2002 (consolidated version), https://e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/asr

[3] Ibid

[4] FATF. FATF Ministers give FATF an open-ended Mandate. Access through URL: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Fatf-mandate.html last accessed: [19/02/2026].

security measures rather than optional compliance tools. In this sense, AML/TF obligations form part of the broader international security architecture, aimed at prevention, disruption and risk containment.

From a macroeconomic perspective, weaknesses in AML/TF frameworks can become systemically destabilising. Illicit financial flows can undermine financial institutions, trigger capital flight, reduce investor confidence, weaken fiscal capacity and isolate jurisdictions from the global financial system[5]. When these effects materialise, they directly erode economic resilience and the state's ability to perform core functions, translating financial fragility into national vulnerability—an outcome explicitly highlighted in national security planning.

A key conceptual question is whether AML/TF should be understood as a direct component of national security or as an indirect contributor to it. While AML/TF measures are primarily designed to protect the financial system from criminal misuse, operational practice demonstrates that this distinction is often artificial. Financial controls routinely detect and disrupt activities that are not primarily profit-driven but strategically motivated—such as the financing of terrorism, sanctions evasion networks, or procurement chains linked to prohibited capabilities. In these cases, AML/TF operates as an early-warning and disruption layer within the financial system, frequently preceding visible security incidents.

This role is amplified in contemporary hybrid threat environments. The same mechanisms used for money laundering—opaque ownership structures, layered transactions, trade-based schemes and cross-border intermediaries—also enable sanctions evasion and the financing of hostile or destabilising activities. As a result, AML/TF frameworks cannot be treated as a standalone compliance regime. They function alongside sanctions implementation, fraud prevention, supervision and intelligence-sharing as part of a single financial integrity and resilience ecosystem.

Accordingly, AML/TF should be understood as a preventive security function. By reducing the permissiveness of the financial system, AML/TF measures limit hostile actors' access to financial infrastructure, increase the costs of illicit activity and strengthen the state's capacity to detect and disrupt threats at an early stage. Their effectiveness depends not on formal compliance alone, but on risk-based implementation, effective supervision, timely information exchange and close integration with sanctions enforcement and broader security governance. Where these elements are strong, the financial system becomes part of the first line of defence; where they are weak, it becomes an enabling environment for hostile activity.

Fraud as a National and Economic Security Threat

Large-scale financial fraud schemes—including investment fraud, romance scams, impersonation fraud, identity theft and money mule networks—have become one of the primary revenue streams for organised criminal groups. Proceeds generated through these activities are systematically reinvested into sustaining criminal infrastructures, facilitating money laundering and enabling further serious financial crime. Europol threat assessments consistently identify fraud as one of the fastest-growing and most profitable forms of organised crime, increasingly intertwined with cyber-enabled activities and complex financial laundering mechanisms.[6]

[5] IMF. IMF and the fight against Money Laundering and Terrorist financing. Access through URL: https://www.imf.org/en/about/factsheets/sheets/2023/fight-against-money-laundering-and-terrorism-financing, last accessed: [19/02/2026].

[6] Europol (2025). *Serious and Organised Crime Threat Assessment (SOCTA), https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf*

From a security perspective, the scale and profitability of fraud elevate it beyond conventional criminality. Fraud-derived revenues contribute to the resilience and adaptability of criminal networks, enabling them to expand operations across jurisdictions and to support activities that directly undermine economic stability and public security.

Contemporary fraud schemes are predominantly cyber-enabled and rely on a combination of digital tools, social engineering techniques, impersonation of public authorities or financial institutions, and manipulation of data and information environments. These methods align closely with established definitions of hybrid threats, which involve the coordinated use of non-military means to exploit societal vulnerabilities and weaken state resilience.[7]

The NATO Strategic Concept (2022) explicitly recognises that economic, cyber and financial activities form an integral part of the modern security environment, alongside military threats. In this context, fraudulent financial operations—alongside sanctions evasion and other forms of economic abuse—can be understood as components of broader hybrid threat ecosystems, where financial systems are exploited to achieve strategic effects without the use of armed force.

Beyond direct financial harm, large-scale fraud has a corrosive impact on public trust, particularly where criminal actors impersonate state institutions, financial authorities or law-enforcement bodies, or deliberately target socially vulnerable groups. Persistent fraud campaigns, combined with perceptions of impunity, undermine confidence in the state's ability to protect citizens and enforce the rule of law.[8]

From a national security perspective, declining trust in public institutions weakens societal resilience to disinformation, complicates crisis management, and erodes state authority. These dynamics are explicitly recognised in national security strategies, including Lithuania's National Security Strategy (2021), which identifies economic security and public trust in institutions as essential preconditions for national security[9].

Given its scale, cross-border nature and systemic impact, fraud prevention cannot be treated solely as a law-enforcement or compliance issue. European Union security frameworks increasingly emphasise that financial crime prevention is integral to economic resilience and internal security. The EU Security Union Strategy 2020–2025 highlights the need for a comprehensive approach to evolving threats, including organised crime, cyber threats and hybrid activities enabled by technological and economic interdependencies.[10]

Similarly, the European Economic Security Strategy underscores that economic vulnerabilities and illicit financial activities can translate into direct security risks for the Union, even where such activities are not explicitly framed as traditional security threats.[5] Within this framework, fraud prevention emerges as a preventive security function, aimed at protecting the integrity of financial systems, limiting the resources available to hostile actors, and reinforcing societal trust and resilience.[11]

---

[7] NATO (2022). NATO Strategic Concept. https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

[8] Lithuanian Parliament (Seimas), *National Security Strategy of the Republic of Lithuania*, Resolution No. IX-907 of 28 May 2002 (consolidated version), https://e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/asr

[9] Ibid

[10] European Commission (2020). *EU Security Union Strategy 2020–2025.* https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[11] European Commission and High Representative (2023). *European Economic Security Strategy.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

Sanctions as an Instrument of National and Collective Security

From a national security perspective, sanctions implementation constitutes a first line of defence within the financial system and a core component of modern security policy. Failures in sanctions enforcement do not merely weaken foreign policy objectives but directly expose states to security risks by enabling hostile actors to access capital, procure restricted goods and sustain destabilising activities. In this sense, sanctions evasion represents not a compliance issue, but a form of strategic leakage that undermines collective security in a manner comparable to deficiencies in cyber defence or border control systems.

Restrictive measures are designed to safeguard international peace and security while influencing the behaviour of states, groups or individuals without recourse to military force. As set out in the Council's 2004 Basic Principles on the Use of Restrictive Measures, sanctions aim to maintain and restore international peace and security in accordance with the principles of the United Nations Charter and the European Union's Common Foreign and Security Policy. These principles include the prevention of threats to peace, respect for territorial integrity, and the promotion and protection of human rights. Sanctions therefore function as a preventive and corrective security instrument, positioned between diplomacy and the use of force.[12][13]

The United Nations' mandate to prevent threats to international peace and security inherently encompasses the objective of non-proliferation of weapons of mass destruction. This commitment provides the legal and normative foundation for UN and EU sanctions regimes targeting nuclear and missile programmes, notably in relation to Iran and North Korea. In these contexts, sanctions seek to constrain access to finance, technology and materials essential to the development of prohibited capabilities, thereby reducing systemic risks to regional and global security.[14][15]

Contemporary sanctions regimes reflect an evolving understanding of security threats. Recognising that threats to peace and stability increasingly originate beyond traditional state actors, sanctions are routinely applied to non-state entities, including terrorist organisations, armed groups and private military companies. Such actors rely heavily on transnational financial networks, logistical chains and access to international markets. Targeted sanctions aim to disrupt these enablers, limiting their operational capacity and reducing their ability to sustain violence, conduct proxy warfare or undermine governance structures.

The scope of sanctions is deliberately broad and adaptable, encompassing a range of restrictive measures tailored to specific threat profiles. These include arms embargoes, restrictions on the export of military and dual-use goods, and prohibitions on equipment that can be used for internal repression.

---

[12] Council of the European Union (2004). Basic Principles on the Use of Restrictive Measures (Sanctions). https://data.consilium.europa.eu/doc/document/ST-10198-2004-INIT/en/pdf

[13] United Nations (1945). *Charter of the United Nations and Statute of the International Court of Justice.* https://treaties.un.org/doc/publication/ctc/uncharter.pdf

[14] European Parliament Research Service (2024). EU sanctions: How they work and challenges for effective implementation. EPRS Briefing, PE 760.416. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760416/EPRS_BRI%282024%29760416_EN.pdf

[15] European Parliament Research Service (2023). EU sanctions and non-proliferation: responding to nuclear threats. EPRS Briefing, PE 751.409. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751409/EPRS_BRI%282023%29751409_EN.pdf

Financial measures play a particularly central role and include asset freezes, travel bans, restrictions on access to capital markets, prohibitions on certain financial transactions, and bans on dealings with designated entities, including central banks. Sectoral sanctions and investment bans further seek to curtail long-term revenue streams, strategic dependencies and the economic foundations of hostile activity.[16]

From a security standpoint, the effectiveness of sanctions is determined not only by their formal adoption but by their implementation within financial and economic systems. Sanctions are intended to deny hostile actors access to the financial infrastructure that enables aggression, proliferation, terrorism and hybrid operations. Where implementation is inconsistent or enforcement mechanisms are weak, sanctioned actors can exploit regulatory gaps, intermediaries and jurisdictional fragmentation to evade restrictions. Such evasion undermines the strategic intent of sanctions and creates vulnerabilities within national and collective security architectures.[17]

Accordingly, sanctions implementation must be understood as an integral component of financial integrity and security governance. It requires close integration with anti-money laundering and counter-terrorist financing frameworks, effective supervision, timely information sharing and sustained cooperation between public authorities, financial institutions and international partners. In this context, sanctions operate at the intersection of economic governance and national security, reinforcing the role of resilient and well-protected financial systems as a foundational element of collective defence.[18]

Conclusions

Financial systems have become a critical domain of modern security. This document demonstrates that money laundering, terrorist financing, large-scale fraud and sanctions evasion are not isolated criminal activities, but interconnected mechanisms that enable hostile actors to finance operations, circumvent restrictions and undermine economic stability and democratic resilience. As such, financial crime must be understood not only as a compliance challenge, but as a structural component of contemporary security threats.

The analysis highlights that AML/CTF frameworks, fraud prevention and sanctions implementation together form an integrated financial integrity system that functions as a preventive security layer. These instruments operate not only to detect and respond to illicit activity, but to constrain access to financial infrastructure, increase the cost of hostile operations and enable early disruption of threats. Their role is particularly significant in hybrid threat environments, where financial, cyber and informational tools are combined to achieve strategic objectives without the use of conventional force.

At both European and national levels, this perspective is increasingly reflected in security frameworks. The European Union's economic and security strategies recognise the interdependence of financial systems and security outcomes, while Lithuania's National Security Strategy explicitly acknowledges the growing importance of economic and financial resilience. This convergence underscores the need to treat financial integrity as a core pillar of national and collective security.

[16] European Commission. EU Sanctions – Restrictive Measures: Overview and related resources. https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en

[17] Financial Action Task Force (FATF) (2023). Complex Proliferation Financing and Sanctions Evasion Schemes. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf

[18] Lund University (2022). Sanctions, Financial Crime and National Security. https://lup.lub.lu.se/luur/download?fileOId=9199862&func=downloadFile&recordOId=9199861

However, the effectiveness of this pillar depends not on formal regulatory frameworks alone, but on their practical implementation. Weak supervision, fragmented information sharing and inconsistent sanctions enforcement create systemic vulnerabilities that can be exploited by hostile actors.

Conversely, risk-based implementation, timely data exchange and close cooperation between public authorities, financial institutions and international partners significantly enhance the capacity to detect, prevent and disrupt threats.

The findings of this document lead to a clear conclusion: financial systems must be treated as part of the first line of defence. Strengthening AML/CTF measures, advancing fraud prevention and ensuring robust sanctions implementation are not only regulatory priorities, but essential security functions. A resilient financial system limits the operational space of hostile actors and reinforces the state's ability to protect its economic stability, institutional integrity and national security in an increasingly complex and interconnected threat environment.